

# SPHEREON 4300

McDATA®  
Sphereon™ 4300 Fabric Switch  
Installation and Service Manual

P/N 620-000171-030  
REV A

## Simplifying Storage Network Management

## Record of Revisions and Updates

Revision	Date	Description
620-000171-000	8/2003	General availability (GA) release of the manual.
620-000171-010	12/2003	Revision of the manual to describe Release 6.1 of the Enterprise Operating System.
620-000171-020	1/2005	Revision of the manual to describe Release 7.0 of the Enterprise Operating System.
620-000171-030	7/2005	Revision of the manual to describe Release 8.0 of the Enterprise Operating System.

**Copyright © 2002, 2005 McDATA Corporation. All rights reserved.**

Printed July 2005

Fourth Edition

No part of this publication may be reproduced or distributed in any form, or by any means, or stored in a database or retrieval system without prior written consent from McDATA Corporation.

The information contained in this document is subject to change without notice. McDATA Corporation assumes no responsibility for any errors that may appear.

All computer applications (including but not limited to microcode) described in this publication are furnished under a license, and may be used or copied only in accordance with the terms of such license. McDATA owns or has the right to license the applications described in this publication. McDATA Corporation retains all rights, title, and interest in the applications.

McDATA Corporation makes no warranties, expressed or implied, by operation of law or otherwise, relating to this publication, and the products or applications described herein. McDATA CORPORATION DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall McDATA Corporation be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data, or profits, arising out of use of this publication, even if advised of the possibility of such damages.

Preface .....	xi
<b>Chapter 1</b>	<b>General Information</b>
Switch Description.....	1-1
Field-Replaceable Units .....	1-2
SFP Transceiver .....	1-3
Power Supply .....	1-4
Controls, Connectors, and Indicators .....	1-4
IML/RESET Button .....	1-4
Ethernet LAN Connector.....	1-5
Power and System Error LEDs .....	1-5
FRU Status LEDs.....	1-5
Maintenance Port.....	1-6
Switch Specifications .....	1-6
Maintenance Approach.....	1-7
Switch Management.....	1-8
Error-Detection, Reporting, and Serviceability Features .....	1-8
Tools and Test Equipment.....	1-9
Tools Supplied with the Product .....	1-10
Tools Supplied by Service Personnel .....	1-11
<b>Chapter 2</b>	<b>Installation Tasks</b>
Factory Defaults .....	2-1
Summary of Installation Tasks.....	2-2
Task 1: Verify Installation Requirements .....	2-2

Task 2: Unpack, Inspect, and Install the Product .....	2-3
Unpack and Inspect Switch.....	2-3
Desktop Installation .....	2-4
Rack-Mount Installation .....	2-5
Task 3: Configure Product at the EFCM Basic Edition Interface	2-6
Configure Product Identification .....	2-7
Configure Date and Time .....	2-8
Configure Parameters .....	2-9
Configure Fabric Parameters .....	2-11
Configure Network Information.....	2-12
Configure Basic Port Information .....	2-14
Configure Port BB_Credit.....	2-15
Configure Port NPIV.....	2-16
Configure SNMP .....	2-16
Enable CLI .....	2-17
Enable or Disable Host Control.....	2-18
Configure SSL Encryption.....	2-19
Install PFE Keys (Optional).....	2-20
Configure Interswitch Links .....	2-22
Task 4: Configure Product Network Information (Optional)...	2-23
Task 5: Cable Fibre Channel Ports.....	2-26
Task 6: Configure Zoning (Optional) .....	2-26
Task 7: Connect Product to a Fabric Element (Optional) .....	2-27
Task 8: Register with the McDATA File Center .....	2-28

## Chapter 3 Maintenance Analysis Procedures

Factory Defaults .....	3-1
Quick Start .....	3-2
MAP 0000: Start MAP .....	3-5
MAP 0100: Power Distribution Analysis .....	3-9
MAP 0200: POST Failure Analysis.....	3-10
MAP 0300: Loss of Browser PC Communication.....	3-11
MAP 0400: FRU Failure Analysis .....	3-14
MAP 0500: Port Failure or Link Incident Analysis .....	3-16
MAP 0600: Fabric or ISL Problem Analysis.....	3-27

## Chapter 4 Repair Information

Procedural Notes .....	4-1
Power On Switch .....	4-2
Power Off Switch.....	4-3

	IML or Reset Switch.....	4-3
	IML.....	4-4
	Reset.....	4-4
	Clean Fiber-Optic Components.....	4-4
	Download Firmware from the Filecenter.....	4-6
	Port LED Diagnostics.....	4-8
	Repair Procedures - EFCM Basic Edition.....	4-9
	Obtain Log Information.....	4-9
	Perform Port Diagnostics.....	4-12
	Collect Maintenance Data.....	4-18
	Set Online State.....	4-19
	Block or Unblock a Port.....	4-20
	Upgrade Firmware.....	4-21
	Manage Configuration Data.....	4-23
<b>Chapter 5</b>	<b>Removal and Replacement Procedures</b>	
	Procedural Notes.....	5-1
	ESD Procedures.....	5-2
	Field-Replaceable Units.....	5-2
	RRP 1: SFP Optical Transceiver.....	5-3
<b>Chapter 6</b>	<b>Illustrated Parts Breakdown</b>	
	Front-Accessible FRUs.....	6-2
	Miscellaneous Parts.....	6-3
	Power Cords and Receptacles.....	6-4
<b>Appendix A</b>	<b>Event Code Tables</b>	
	System Events (000 through 199).....	A-2
	Fan Events (300 through 399).....	A-21
	CTP Card Events (400 through 499).....	A-25
	Port Events (500 through 599).....	A-31
	Thermal Sensor Events (800 through 899).....	A-40
	<b>Index.....</b>	<b>I-1</b>



1-1	Sphereon 4300 Switch (Front View) .....	1-2
1-2	Sphereon 4300 Switch (Rear View) .....	1-3
1-3	Door Key .....	1-10
1-4	Loopback Plug .....	1-10
1-5	Fiber-Optic Protective Plug .....	1-10
1-6	Null Modem Cable .....	1-11
2-1	Hardware View .....	2-7
2-2	Identification View .....	2-7
2-3	Date Time View .....	2-8
2-4	Parameters View .....	2-9
2-5	Fabric Parameters View .....	2-11
2-6	Network View .....	2-13
2-7	Basic Information View .....	2-14
2-8	SNMP View .....	2-16
2-9	CLI View .....	2-18
2-10	OSMS View .....	2-18
2-11	SSL View .....	2-19
2-12	Maintenance Feature Installation View .....	2-21
2-13	Connection Description Dialog Box .....	2-24
2-14	McDATA Filecenter Home Page .....	2-29
4-1	Clean Fiber-Optic Components .....	4-5
4-2	McDATA Filecenter Home Page .....	4-6
4-3	Port List View .....	4-12
4-4	Diagnostics View .....	4-16
4-5	System Files View .....	4-18
4-6	Switch View .....	4-20

4-7	Basic Information View .....	4-21
4-8	Firmware Upgrade View .....	4-22
4-9	Backup Configuration View .....	4-24
4-10	Restore Configuration View .....	4-25
5-1	SFP Optical Transceiver Removal and Replacement .....	5-4
6-1	Front-Accessible FRUs .....	6-2
6-2	Miscellaneous Parts .....	6-3
6-3	Power Cords and Receptacles .....	6-4



2-1	Factory-Set Defaults (Product) .....	2-1
2-2	Installation Task Summary .....	2-2
3-1	Factory-Set Defaults .....	3-1
3-2	MAP Summary .....	3-2
3-3	Event Codes versus Maintenance Action .....	3-2
3-4	MAP 200 Event Codes .....	3-10
3-5	MAP 200 Byte 0 FRU Codes .....	3-11
3-6	MAP 400 Event Codes .....	3-15
3-7	MAP 500 Event Codes .....	3-17
3-8	Link Incident Messages .....	3-17
3-9	Invalid Attachment Reasons and Actions .....	3-18
3-10	Inactive Port Reasons and Actions .....	3-23
3-11	MAP 600 Event Codes .....	3-27
3-12	E_Port Segmentation Reasons and Actions .....	3-30
3-13	Port Fence Codes and Actions .....	3-34
3-14	Fabric Merge Failure Reasons and Actions .....	3-36
4-1	Port Operational States .....	4-8
5-1	Concurrent FRU .....	5-2
6-1	Front-Accessible FRU Parts List .....	6-2
6-2	Miscellaneous Parts List .....	6-3
6-3	Power Cord and Receptacle List .....	6-5



This publication is part of a documentation suite that supports the McDATA® Sphereon 4300 Fabric Switch.

## Who Should Use this Manual

Use this publication if you are a trained installation and service representative experienced with the product, storage area network (SAN) technology, and Fibre Channel technology.



## Organization of this Manual

The product contains no customer-serviceable parts that require internal access to the product during normal operation or prescribed maintenance conditions. In addition, refer to this manual for instructions prior to performing any maintenance action.

This publication includes six chapters and one appendix organized as follows:

**Chapter 1, *General Information*** - This chapter describes the switch, including field-replaceable units (FRUs), controls, connectors, and indicators, and switch specifications. The chapter also describes the maintenance approach, error detection and reporting features, serviceability features, software diagnostic features, and tools and test equipment.

**Chapter 2, *Installation Tasks*** - This chapter describes tasks to install, configure, and verify operation of the switch.

**Chapter 3, *Maintenance Analysis Procedures*** - This chapter describes maintenance analysis procedures (MAPs) to fault isolate a switch problem to an individual FRU.

**Chapter 4, *Repair Information*** - This chapter describes supplementary diagnostic and repair procedures for a failed switch. The chapter includes procedures to display and use log information, perform port diagnostics, manage configuration data, collect maintenance data, power-on, power-off, and reset the switch, set the switch online or offline, block ports, manage switch firmware, clean fiber optics, and install or upgrade management server software.

**Chapter 5, *Removal and Replacement Procedures*** - This chapter describes procedures to remove and replace switch FRUs.

**Chapter 6, *Illustrated Parts Breakdown*** - This chapter illustrates, describes, and shows the location of switch FRUs. In addition, switch FRUs are cross-referenced to corresponding part numbers.

**Appendix A, *Event Code Tables*** - This appendix provides an explanation of event codes that appear at the EFCM Basic Edition interface. The event severity and a recommended course of action in response to each event are also provided.

An ***Index*** is also provided.

#### Related Publications

Other publications that provide additional information about the switch include:

- *McDATA Products in a SAN Environment - Planning Manual* (626-000124).
- *McDATA EFCM Basic Edition User Manual* (620-000240).
- *McDATA SNMP Support Manual* (620-000131).
- *McDATA E/OS Command Line Interface User Manual* (620-000134).
- *McDATA Sphereon 4300, 4500, and 4700 Switch Rack-Mount Kit Installation Instructions* (958-000316).
- *McDATA FC-512 Fabriccenter Equipment Cabinet Installation and Service Manual* (620-000100).

#### Ordering Printed Manuals

To order a printed copy of this publication, submit a purchase order as described in *Ordering McDATA Documentation Instructions* at <http://www.mcdata.com>. To obtain documentation CD-ROMs, contact your McDATA sales representative.

**Where to Get Help** For technical support, contact the McDATA solution center. The center provides a point of contact for assistance and is staffed full time, including holidays. Contact the center at the phone number, fax number, or e-mail address listed below. Have the product serial number (printed on the service label) available.

**Phone: (800) 752-4572 or (720) 558-3910**

**Fax: (720) 558-3851**

**E-mail: support@mcddata.com**

Send publication-related comments to the solution center by telephone, fax, or e-mail. Identify page numbers and details.

**Trademarks** The following terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of McDATA Corporation or SANavigator, Inc. in the United States or other countries or both:

<u>Registered Trademarks</u>	<u>Trademarks</u>
Fabricenter®	EON™
HotCAT®	OPENconnectors™
McDATA®	Sphereon™
Multi-Capable Storage Network Solutions®	
Networking the World's Business Data®	
OPENready®	
SANtegrity®	

All other trademarked terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of their respective owners in the United States or other countries or both.

### Laser Compliance Statement



Product laser transceivers are tested and certified in the United States to conform to Title 21 of the Code of Federal Regulations (CFR), Subchapter J, Parts 1040.10 and 1040.11 for Class 1 laser products. Transceivers are tested and certified to be compliant with International Electrotechnical Commission IEC825-1 and European Norm EN60825-1 and EN60825-2 regulations for Class 1 laser products. Class 1 laser products are not considered hazardous. The transceivers are designed to prevent human access to laser radiation above a Class 1 level during normal operation or prescribed maintenance conditions.

### Federal Communications Commission (FCC) Statement

Products generate, use, and can radiate radio frequency energy, and if not installed and used in accordance with instructions provided, may cause interference to radio communications. Products are tested and found to comply with the limits for Class A and Class B computing devices pursuant to Subpart B of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in a residential environment. Any modification or change made to a product without explicit approval from McDATA, by means of a written endorsement or through published literature, invalidates the service contract and voids the warranty agreement with McDATA.

### Canadian EMC Statements

The statements below indicate product compliance with Interference Causing Equipment Standard (ICES) and Norme sur le Matériel Brouiller (NMB) electromagnetic compatibility (EMC) requirements as set forth in ICES/NMB-003, Issue 4.

- This Class A or Class B digital apparatus complies with Canadian ICES-003.
- Cet appareil numérique de la classe A et classe B est conforme à la norme NMB-003 du Canada.

### United States and Canada UL Certification



The C-UL-US mark on a product indicates compliance with American National Standards Institute (ANSI) and Standards Council of Canada (SCC) safety requirements as tested, evaluated, and certified by Underwriters Laboratories Inc. (UL) and Underwriters Laboratories of Canada (ULC).

International Safety  
Conformity  
Declaration (CB  
Scheme)



A certification bodies (CB) test report supporting a product indicates safety compliance with the International Electrotechnical Commission (IEC) system for conformity testing and certification of electrical equipment (IECEE) CB scheme.

The CB scheme is a multilateral agreement among participating countries and certification organizations that accepts test reports certifying the safety of electrical and electronic products.

European Union  
Conformity  
Declarations and  
Directives (CE Mark)



The CE mark on a product indicates compliance with the following regulatory requirements as set forth by European Norms (ENs) and relevant international standards for commercial and light industrial information technology equipment (ITE):

- **EN55022: 1998** - ITE-generic radio frequency interference (RFI) emission standard for domestic, commercial, and light industrial environments, including electrical business equipment.
- **EN55024-1: 1998** - ITE-generic electromagnetic immunity standard for domestic, commercial, and light industrial environments, including electrical business equipment.
- **EN60950/A11:1997** - ITE-generic electrical and fire safety standard for domestic, commercial, and light industrial environments, including electrical business equipment.
- **EN61000-3-2:1995** - ITE-generic harmonic current emissions standard for domestic, commercial, and light industrial environments (equipment with rated current less than or equal to 16 amperes per phase).
- **EN61000-3-3:1995** - ITE-generic voltage fluctuation and flicker standard (low-voltage power supply systems) for domestic, commercial, and light industrial environments (equipment with rated current less than or equal to 16 amperes per phase).

In addition, the European Union (EU) Council has implemented a series of directives that define product safety standards for member countries. The following directives apply:

- Products conform with all protection requirements of EU directive **89/336/EEC** (Electromagnetic Compatibility Directive) in accordance with the laws of the member countries relating to EMC emissions and immunity.

- Products conform with all protection requirements of EU directive **73/23/EEC** (Low-Voltage Directive) in accordance with the laws of the member countries relating to electrical safety.
- Products conform with all protection requirements of EU directive **93/68/EEC** (Machinery Directive) in accordance with the laws of the member countries relating to safe electrical and mechanical operation of the equipment.

McDATA does not accept responsibility for any failure to satisfy the protection requirements of any of these directives resulting from a non-recommended or non-authorized modification to a product.

#### European Union EMC and Safety Declaration (N-Mark)



The N-mark on a product indicates compliance with European Union EMC and safety requirements as tested, evaluated, and certified by the Norwegian Board for Testing and Approval of Electrical Equipment (Norges Elektriske Materiellkontroll or NEMKO) laboratory or a NEMKO-authorized laboratory.

#### Argentina IRAM Certification



The Instituto Argentino de Normalización (IRAM) S-mark on a product indicates compliance with Dirección Nacional de Comercio Interior (DNCI) Resolution Number 92/98, Phase III (for information technology equipment safety). In conjunction with the S-mark is the AR-UL mark, certified by UL de Argentina, S.R.L., and accredited by the Argentine Accreditation Organization (OAA).

#### Australia and New Zealand C-Tick Mark



The Australia and New Zealand regulatory compliance mark (C-tick mark) on a product indicates compliance with regulatory requirements for EMC (for information technology equipment) as set forth by the Australian Communications Authority (ACA) and the Radio Spectrum Management Group (RSM) of New Zealand.



People's Republic of  
China CCC Mark



The China Compulsory Certification mark (CCC mark) on a product indicates compliance with People's Republic of China regulatory requirements for safety and EMC (for information technology equipment) as set forth by the National Regulatory Commission for Certification and Accreditation.

Chinese National  
Standards Statement

The Chinese National Standards (CNS) statement below indicates product compliance with Taiwanese Bureau of Standards, Metrology, and Inspection (BSMI) regulatory requirements. The statement indicates a product is a Class A or Class B product, and in a domestic environment may cause radio interference, in which case the user is required to take corrective actions.

這是乙類的資訊產品，在居住環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

German TÜV GS Mark



The German regulatory compliance mark (TÜV GS Mark) on a product indicates compliance with the German Safety of Equipment Act as tested by the Technical Inspection Association (Technischer Überwachungsverein or TÜV), and accredited by the Central Office of Safety of the German Länder (Zentralstelle der Länder für Sicherheit or ZLS).

Japanese VCCI  
Statement

The Voluntary Control Council for Interference (VCCI) statement below applies to information technology equipment, and indicates product compliance with Japanese regulatory requirements. The statement indicates a product is a Class A or Class B product, and in a domestic environment may cause radio interference, in which case the user is required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラスB情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## Korean MIC Mark



The Korean Ministry of Information and Communications mark (MIC mark) on a product indicates compliance with regulatory requirements for safety and EMC (for information technology equipment) as authorized and certified by the Korean Radio Research Institute (RRI).

## Mexican NOM Mark



The Official Mexican Standard (Normas Oficiales Mexicanas or NOM) mark on a product indicates compliance with regulatory requirements for safety (for information technology equipment) as authorized and accredited by the National System of Accreditation of Testing Laboratories (Sistema Nacional de Acreditamiento de Laboratorios de Pruebas or SINALP).

## Russian GOST Certification



The Russian Gosudarstvennyi Standart (GOST) mark on a product indicates compliance with regulatory requirements for safety and EMC (for information technology equipment) as authorized and accredited by the State Committee for Standardization, Metrology and Certification.

## Danger and Attention Statements

The following **DANGER** statement appears in this publication and describes a safety practice that must be observed while installing or servicing a product. A **DANGER** statement provides essential information or instructions for which disregard or noncompliance may result in death or severe personal injury. The statement appears in English, followed by translations to:

- Chinese (simplified - People's Republic of China).
- Chinese (traditional - Taiwan).
- French (European).
- German.
- Hebrew.
- Italian.

- Portuguese.
- Spanish (European).
- Spanish (Latin American).



### **DANGER**

***Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.***



### **危險**

***使用所提供的電源線。確保使用正確型號的設備電源插座，提供必需的電壓並且正確接地。***



### **危險**

***使用隨附的電源線，確定使用正確類型的設備電源插座，提供必需的電壓，並且正確接地。***



### **DANGER**

***Utiliser les câbles d'alimentation fournis. S'assurer que la prise de courant du local est du type correct, délivre la tension requise et est correctement raccordée à la terre.***



### **GEFAHR**

***Die mitgelieferten Netzkabel verwenden. Sicherstellen, dass die verwendete Netzsteckdose dem vorgeschriebenen Typ entspricht, die erforderliche Spannung liefert und einwandfrei geerdet ist.***

## סכנה



השתמש בכבלי החשמל הנלווים. וודא כי כלי הקיבול לחשמל של המתקן הוא מהסוג הנכון, מספק את המתח הדרוש, ומוארק כהלכה.



### PERICOLO

***Usare il cavo di alimentazione in dotazione. Assicurarsi che la presa di corrente a disposizione sia del tipo corretto, eroghi la tensione richiesta e sia dotata di messa a terra idonea.***



### PERIGO

***Use os cordões elétricos fornecidos. Certifique-se de que o tipo de receptor de energia da facilidade é apropriado, fornece a voltagem necessária, e está corretamente aterrado.***



### PELIGRO

***Utilice los cables de alimentación proporcionados. Asegúrese que el receptáculo tomacorriente para la instalación sea el tipo correcto, suministre el voltaje necesario, y que esté apropiadamente puesto a tierra.***



### PELIGRO

***Utilice los cables de alimentación proporcionados. Asegúrese que el receptáculo tomacorriente para la instalación sea del tipo correcto, suministre el voltaje necesario, y que esté apropiadamente conectado a tierra.***

The following **ATTENTION** statements appear in this publication and describe practices that must be observed while installing or servicing the switch. An **ATTENTION** statement provides essential information or instructions for which disregard or noncompliance may result in equipment damage or loss of data.

---

**ATTENTION !** Prior to servicing a product, determine the Ethernet LAN configuration. Installation of products on a public customer intranet can complicate problem determination and fault isolation.

---

---

**ATTENTION !** A reset should only be performed if a CTP card failure is indicated. Do not reset a managed product unless directed to do so by a procedural step or the next level of support.

---

**General Precautions** When installing or servicing the product, follow these practices:

- Always use correct tools.
- Always use correct replacement parts.
- Keep all paperwork up to date, complete, and accurate.

**ESD Precautions** Follow these electrostatic discharge (ESD) procedures:

- If the product is connected to facility power (grounded), wear an ESD wrist strap and grounding cable connected to the product chassis.
- If the product is not connected to facility power (not grounded), wear an ESD wrist strap and grounding cable connected to an approved bench grounding point.
- Touch the product chassis once before performing a procedure, and once each minute during the procedure.
- Store ESD-sensitive FRUs in antistatic packaging.



The McDATA® Sphereon™ 4300 Fabric Switch provides 12 ports of low-cost and high-performance dynamic Fibre Channel connectivity for switched fabric or arbitrated loop devices. This function allows low-cost, low-bandwidth workgroup (edge) devices to communicate with mainframe servers, mass storage devices, or other peripherals, and ultimately be incorporated into an enterprise storage area network (SAN) environment. This chapter describes:

- The switch, including field-replaceable units (FRUs), controls, connectors, indicators, and specifications.
- Maintenance approach.
- Switch management.
- Error detection, reporting, and serviceability features.
- Tools and test equipment.

---

## Switch Description

The switch provides Fibre Channel connectivity through generic mixed ports (GX\_Ports). Ports operate at 1.0625 or 2.1250 gigabits per second (Gbps), and can be configured as:

- Fabric ports (F\_Ports) to provide direct connectivity for switched fabric devices.

- Expansion ports (E\_Ports) to provide interswitch link (ISL) connectivity to fabric directors and switches.
- Fabric loop ports (FL\_Ports) to provide connectivity and fabric attachment for Fibre Channel arbitrated loop (FC-AL) devices.

The switch is installed on a table or desktop, mounted in an FC-512 Fabriccenter® equipment cabinet, or mounted in any standard 19-inch equipment rack.

Operators with a browser-capable PC and Internet connectivity can manage the switch through a firmware-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface. The interface manages only a single switch, and provides a graphical user interface (GUI) that supports configuration, statistics monitoring, operation, and maintenance. The interface is opened from a web browser running Netscape Navigator® 4.6 (or higher) or Microsoft® Internet Explorer 4.0 (or higher).

### Field-Replaceable Units

The switch provides a modular design that enables quick removal and replacement of FRUs, including small form factor pluggable (SFP) optical transceivers and power supply assemblies. [Figure 1-1](#) illustrates the front of the switch and shows the:

1. Ethernet LAN connector.
2. Initial machine load and reset (IML/RESET) button.
3. Green power (PWR) light-emitting diode (LED).
4. Amber system error (ERR) LED.
5. SFP optical transceivers (12).

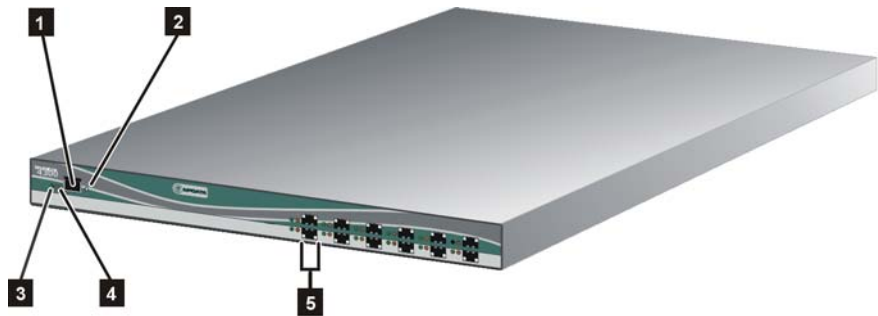


Figure 1-1 Sphereon 4300 Switch (Front View)

112M1010



Figure 1-2 illustrates the rear of the switch and shows the:

1. AC power receptacle.
2. RS-232 maintenance port.



Figure 1-2 Sphereon 4300 Switch (Rear View)

i12M1011

## SFP Transceiver

Singlemode or multimode fiber-optic cables attach to switch ports through SFP transceivers. The fiber-optic transceivers provide duplex LC<sup>®</sup> connectors, and can be detached from switch ports (through a 10-pin interface) for easy replacement. The following fiber-optic transceiver types are available:

- **Dual-rate shortwave laser (1.0625 or 2.1250 Gbps)** - Shortwave laser transceivers (850 nm) provide connectivity:
  - At 500 meters (1.0625 Gbps) through 50-micron multimode fiber-optic cable.
  - At 300 meters (2.1250 Gbps) through 50-micron multimode fiber-optic cable.
  - At 300 meters (1.0625 Gbps) through 62.5-micron multimode fiber-optic cable.
  - At 150 meters (2.1250 Gbps) through 62.5-micron multimode fiber-optic cable.
- **Dual-rate longwave laser (1.0625 or 2.1250 Gbps)** - Longwave laser transceivers (1310 nm) provide connectivity at 10 kilometers through 9-micron singlemode fiber-optic cable.
- **Dual-rate extended longwave laser (1.0625 or 2.1250 Gbps)** - Longwave laser transceivers (1310 nm) provide connectivity at 20 or 35 kilometers through 9-micron singlemode fiber-optic cable.

The switch also provides a predictive optics monitoring (POM) feature that monitors operation of SFP optical transceivers. Digital diagnostics-enabled optical transceivers report temperature, voltage current, transceiver power, and receiver power to product firmware. Optical transceivers also provide vendor-specific threshold values for these parameters.

---

## Power Supply

The switch contains one power supply with two internal cooling fans. The assembly is not a FRU. The power supply steps down and rectifies facility input power to provide 3.3 volts direct current (VDC), 5 VDC, and 12 VDC to the control processor (CTP) card. The power supply also provides input filtering, overvoltage protection, and overcurrent protection, and is input rated at 90 to 264 volts alternating current (VAC).

Three cooling fans (two integrated in the power supply) provide cooling for the power supply and CTP card, as well as redundancy for continued operation if a single fan fails.

---

## Controls, Connectors, and Indicators

Controls, connectors, and indicators for the switch include the:

- **IML/RESET** button.
- Ethernet LAN connector.
- Green **PWR** and amber **ERR** LEDs.
- Green, blue, and amber status LEDs associated with FRUs.
- RS-232 maintenance port.

---

## IML/RESET Button

When the **IML/RESET** button is pressed, held for three seconds, and released, the switch performs an IML that reloads the firmware from FLASH memory. This operation is not disruptive to Fibre Channel traffic. When the **IML/RESET** button is pressed and held for ten seconds, the switch performs a reset. After three seconds, the **ERR** LED blinks at twice the unit beaconing rate. A reset is disruptive to Fibre Channel traffic and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.

- Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

Perform a reset only if a CTP card failure is indicated. The button is flush mounted to protect against inadvertent activation.

---

### Ethernet LAN Connector

The front panel has a 10/100 megabit per second (Mbps) RJ-45 twisted-pair connector that attaches to an Ethernet LAN to provide communication with a management server or simple network management protocol (SNMP) workstation.

The connector provides two green LEDs. The left LED illuminates to indicate LAN operation at 10 Mbps. The right LED illuminates to indicate operation at 100 Mbps.

---

### Power and System Error LEDs

The **PWR** LED illuminates when the switch is connected to facility AC power and is operational (the product does not have a power switch). If the LED extinguishes, a facility power source, power cord, or power distribution failure is indicated.

The **ERR** LED illuminates when the switch detects an event requiring operator attention, such as a FRU failure. The LED illuminates as long as an event is active. The LED extinguishes when *Clear System Error Light* is selected from the EFCM Basic Edition interface. The **ERR** LED also blinks if unit beaconing is enabled. An illuminated LED (indicating a failure) takes precedence over unit beaconing.

---

### FRU Status LEDs

Amber and green/blue LEDs associated with switch FRUs provide status information as follows:

- **Fibre Channel ports** - LEDs to the left of each port illuminate, extinguish, or blink to indicate port status and speed. The amber LED illuminates if the port fails. The green/blue LED illuminates green to indicate 1.0625 Gbps port operation. The green/blue LED illuminates blue to indicate 2.1250 Gbps port operation.
- **Power supply assembly** - An amber LED on each assembly illuminates if the FRU fails.

---

## Maintenance Port

The rear panel has a 9-pin DSUB maintenance port that provides a connection for a local terminal or dial-in connection for a remote terminal. The port is typically used only by maintenance personnel, however operators can use the port to configure network addresses.

---

## Switch Specifications

This section lists physical characteristics, storage and shipping environment, operating environment, and service clearances.

### Physical Characteristics

#### Dimensions:

**Height:** 4.1 centimeters (1.6 inches) or 1 rack unit

**Width:** 43.7 centimeters (17.2 inches)

**Depth:** 47.3 centimeters (18.6 inches)

**Weight:** 6.8 kilograms (15.0 pounds)

#### Power requirements:

**Input voltage:** 90 to 264 VAC

**Input current:** 0.4 amps at 208 VAC

**Input frequency:** 47 to 63 Hz

#### Heat dissipation:

37 watts (127 BTUs/hr)

#### Cooling airflow clearances (switch chassis):

**Right and left side:** 1.3 centimeters (0.5 inches)

**Front and rear:** 7.6 centimeters (3.0 inches)

**Top and bottom:** No clearance required

#### Shock and vibration tolerance:

60 Gs for 10 milliseconds without nonrecoverable errors

#### Acoustical noise:

64 dB "A" scale

#### Inclination:

10<sup>0</sup> maximum

**Storage and Shipping Environment**

Protective packaging must be provided to protect the switch under all shipping methods (domestic and international).

**Shipping temperature:**

-40<sup>0</sup> F to 140<sup>0</sup> F (-40<sup>0</sup> C to 60<sup>0</sup> C)

**Storage temperature:**

34<sup>0</sup> F to 140<sup>0</sup> F (1<sup>0</sup> C to 60<sup>0</sup> C)

**Shipping relative humidity:**

5% to 100%

**Storage relative humidity:**

5% to 80%

**Maximum wet-bulb temperature:**

84<sup>0</sup> F (29<sup>0</sup> C)

**Altitude:**

40,000 feet (12,192 meters)

**Operating Environment****Temperature:**

40<sup>0</sup> F to 104<sup>0</sup> F (4<sup>0</sup> C to 40<sup>0</sup> C)

**Relative humidity:**

8% to 80%

**Maximum wet-bulb temperature:**

81<sup>0</sup> F (27<sup>0</sup> C)

**Altitude:**

10,000 feet (3,048 meters)

---

## Maintenance Approach

The maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting product operation or associated applications. Fault isolation begins when one or more of the following occur:

- Event information displays at a browser-capable PC communicating with the product through the EFCM Basic Edition interface.
- LEDs on the product front panel or FRUs illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.
- Event notification is received at a designated support center through an e-mail message or the call-home feature.

Fault isolation and repair information is provided through maintenance analysis procedures (MAPs). MAPs are step-by-step procedures that provide information to interpret events, isolate a failure to a FRU, remove and replace the FRU, and verify product operation. Fault isolation begins with *MAP 0000: Start MAP*.

---

## Switch Management

The switch is managed and controlled through a customer-supplied PC platform with Internet communication to the product-resident EFCM Basic Edition interface. This graphical user interface (GUI) allows service personnel to perform configuration tasks, view system alerts and related log information, and monitor switch status, port status, and performance. FRU status and system alert information are highly visible.

The EFCM Basic Edition interface is opened from a standard web browser running Netscape Navigator<sup>®</sup> Version 4.6 (or higher) or Microsoft Internet Explorer Version 4.0 (or higher). At the browser, enter the IP address of the switch as the Internet uniform resource locator (URL).

---

## Error-Detection, Reporting, and Serviceability Features

The switch provides the following error detection, reporting, and serviceability features:

- LEDs on switch FRUs and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.
- Redundant FRUs (SFP transceivers) that are removed or replaced without disrupting switch or Fibre Channel link operation.

- A modular design that enables quick removal and replacement of FRUs without the use of tools or equipment.
- System alerts and logs that display switch and Fibre Channel link status at the EFCM Basic Edition interface.
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (loopback tests).
- An RS-232 maintenance port at the rear of the switch (port access is password protected) that enables installation or service personnel to change the switch's IP address, subnet mask, and gateway address.

These parameters can also be changed through a Telnet session, access for which is provided through a local or remote PC with an Internet connection to the switch.

- Data collection through the EFCM Basic Edition interface to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.
- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.
- SNMP management using the Fibre Channel Fabric Element MIB, Transmission Control Protocol/Internet Protocol (TCP/IP) MIB-II definition (RFC 1157), or a product-specific private enterprise MIB that runs on the switch. Up to six authorized management workstations can be configured through the EFCM Basic Edition interface to receive unsolicited SNMP trap messages. The trap messages indicate product operational state changes and failure conditions.

---

## Tools and Test Equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the product. These tools are supplied with the product or must be supplied by service personnel.

## Tools Supplied with the Product

The following tools are supplied with the product:

- **Door key** - A door key with 5/16-inch socket ([Figure 1-3](#)) is required to open front and rear doors of the Fabriccenter Equipment Cabinet. A 5/16-inch socket wrench may also be used.



Figure 1-3 Door Key

- **Loopback plug** - A multimode (shortwave laser) or singlemode (longwave laser) loopback plug ([Figure 1-4](#)) is required to perform port diagnostic tests. Loopback plugs are shipped with the product, depending on the types of port transceivers installed.

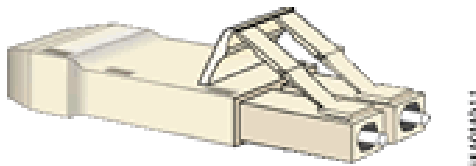


Figure 1-4 Loopback Plug

- **Fiber-optic protective plug** - For safety and port transceiver protection, fiber-optic protective plugs ([Figure 1-5](#)) are inserted in all product ports without fiber-optic cables attached. Products are shipped with protective plugs installed.

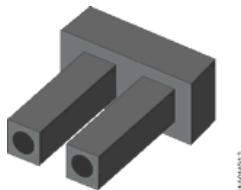


Figure 1-5 Fiber-Optic Protective Plug



- **Null modem cable** - An asynchronous RS-232 null modem cable (Figure 1-6) is required to configure product network addresses and acquire event log information through the product's serial port. The cable has nine conductors and DB-9 female connectors.

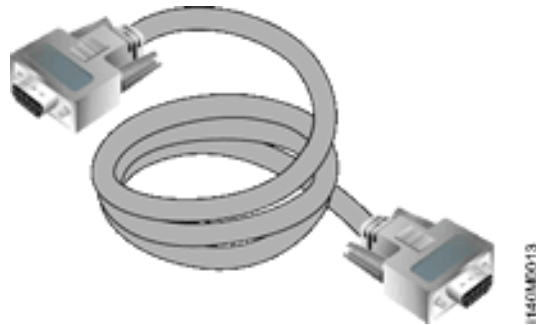


Figure 1-6 Null Modem Cable

## Tools Supplied by Service Personnel

The following tools should be supplied by service personnel:

- **Scissors or pocket knife** - A sharp cutting edge (scissors or knife blade) is required to cut protective strapping when unpacking replacement FRUs.
- **Flat-tip and cross-tip (Phillips) screwdrivers** - Screwdrivers are required to remove, replace, adjust, or tighten FRUs, chassis, or cabinet components.
- **T10 Torx® tool** - The tool is required to rack-mount products or to remove, replace, adjust, or tighten chassis or cabinet components.
- **ESD grounding cable and wrist strap** - An ESD wrist strap is required when working with ESD-sensitive FRUs, including optical transceivers.
- **Maintenance terminal** - A desktop or notebook PC is required to configure product network addresses and acquire event log information through the maintenance port. The PC must have:
  - The Microsoft® Windows® 98, Windows® 2000, Windows® 2003, Windows® XP, or Windows® ME operating system installed.

- RS-232 serial communication software (such as ProComm Plus™ or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.
- **Fiber-optic cleaning kit** - The kit contains tools and instructions to clean fiber-optic cables, connectors, loopback plugs, and protective plugs.

This chapter describes tasks to install, configure, and verify operation of the Sphereon 4300 Fabric Switch using the EFCM Basic Edition interface. The product can be installed on a table top, mounted in a Fabriccenter equipment cabinet, or mounted in any standard 19-inch equipment rack.

## Factory Defaults

[Table 2-1](#) lists factory-set defaults for the product.

Table 2-1 Factory-Set Defaults (Product)

Item	Default
EFCM Basic Edition interface user name (case sensitive)	Administrator
EFCM Basic Edition interface password (case sensitive)	password
Customer-level password (maintenance port access)	password
Maintenance-level password (maintenance port access)	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

## Summary of Installation Tasks

[Table 2-2](#) summarizes installation tasks for the product. The table describes each task, states if the task is optional, and lists the page reference.

Table 2-2 Installation Task Summary

Task Number and Description	Required or Optional	Page
<i>Task 1: Verify Installation Requirements.</i>	Required.	<a href="#">2-2</a>
<i>Task 2: Unpack, Inspect, and Install the Product.</i>	Required.	<a href="#">2-3</a>
<i>Task 3: Configure Product at the EFCM Basic Edition Interface.</i>	Required.	<a href="#">2-6</a>
<i>Task 4: Configure Product Network Information (Optional).</i>	Configure if connecting multiple switches or connecting switch to a public LAN.	<a href="#">2-23</a>
<i>Task 5: Cable Fibre Channel Ports.</i>	Required.	<a href="#">2-26</a>
<i>Task 6: Configure Zoning (Optional).</i>	Perform task to configure zoning.	<a href="#">2-26</a>
<i>Task 7: Connect Product to a Fabric Element (Optional).</i>	Perform task to connect switch to a Fibre channel fabric.	<a href="#">2-27</a>
<i>Task 8: Register with the McDATA File Center.</i>	Required.	<a href="#">2-28</a>

## Task 1: Verify Installation Requirements

Verify the following requirements are met prior to product and management interface installation. Ensure:

- A site plan is prepared, configuration planning tasks are complete, planning considerations are evaluated, and related planning checklists are complete. Refer to *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.
- Fibre Channel SAN design and director, fabric switch, and SAN router device connectivity are evaluated, and the related planning worksheet is complete. Refer to the *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.

- Support is available for a browser-capable PC and Internet connectivity to support the product-resident EFCM Basic Edition interface.
- Support equipment and technical personnel are available for the installation.
- The required number and type of fiber-optic jumper cables are delivered and available. Ensure cables are the correct length and have the required connectors.
- A Fabriccenter cabinet or customer-supplied 19-inch equipment rack and associated hardware are available (optional).
- Remote workstations or simple network management protocol (SNMP) workstations are available (optional). Workstations are customer-supplied and connected through a public or dedicated LAN segment.

---

## Task 2: Unpack, Inspect, and Install the Product

The following paragraphs provide instructions to unpack, inspect, and install one or more switches. If the switch is delivered in a Fabriccenter equipment cabinet, go to [Task 3: Configure Product at the EFCM Basic Edition Interface](#).

---

### Unpack and Inspect Switch

Unpack and inspect switch(es) as follows:

1. Inspect shipping container(s) for damage. If a container is damaged, ensure a freight carrier representative is present when the container is opened. Unpack shipping container(s) and inspect each item for damage. Ensure packaged items correspond to items listed on the enclosed bill of materials.
2. If items are damaged or missing, contact the solution center:

**Phone: (800) 752-4572 or (720) 558-3910**

**Fax: (720) 558-3851**

**E-mail: [support@mcddata.com](mailto:support@mcddata.com)**

---

## Desktop Installation

To install a switch on a desktop:

1. Remove the backing from the four adhesive rubber pads and apply the pads to the underside of the switch. Ensure pads are aligned with the scribed circles at each corner.
2. Position the switch on a table or desktop as directed by the customer. Ensure:
  - A grounded AC electrical outlet is available.
  - Adequate ventilation is present, and areas with excessive heat, dust, or moisture are avoided.
  - All planning considerations are met. Refer to *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.
3. Verify all field-replaceable units (FRUs) are installed as ordered.
4. Connect the AC power cord to the receptacle at the rear of the chassis.
5. Connect the AC power cord to a facility power source that provides single-phase, 100 to 240 volt alternating current (VAC) current.
6. When the power cord is connected, the switch powers on and performs power-on self-tests (POSTs). During POSTs:
  - a. The green power (**PWR**) LED on the front panel illuminates.
  - b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
  - c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
  - d. LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
7. After successful POST completion, the **PWR** LED remains illuminated and all other front panel LEDs extinguish.
8. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) to isolate the problem.
9. Go to [Task 3: Configure Product at the EFCM Basic Edition Interface](#).

## Rack-Mount Installation

Perform the following steps to install and configure the switch in a Fabriccenter cabinet or a customer-supplied equipment rack. An optional rack-mount kit, T10 Torx tool, and #2 Phillips screwdriver are required.

1. Locate the rack-mount position as directed by the customer. The switch is 1.75 inches, or 1U high.
2. Verify all FRUs are installed as ordered.
3. Open the rack-mount kit and inspect the contents. Refer to the enclosed bill of materials and verify all parts are delivered.
4. Using a T10 Torx tool and #2 Phillips screwdriver, install the switch in the equipment cabinet. Refer to *McDATA Sphereon 4300, 4500, and 4700 Switch Rack-Mount Kit Installation Instructions* (958-000316) for guidance.
5. Connect the AC power cord to the receptacle at the rear of the chassis.
6. Connect the AC power cord to a rack power strip connected to a facility power source that provides single-phase, 100 to 240 VAC current.
7. When the power cord is connected, the switch powers on and performs POSTs. During POSTs:
  - a. The green power (**PWR**) LED on the front panel illuminates.
  - b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
  - c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
  - d. LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
8. After successful POST completion, the **PWR** LED remains illuminated and all other front panel LEDs extinguish.
9. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) to isolate the problem.
10. Go to [Task 3: Configure Product at the EFCM Basic Edition Interface](#).

## Task 3: Configure Product at the EFCM Basic Edition Interface

Perform these procedures to configure the product from the EFCM Basic Edition interface. A browser-capable PC with Internet or Ethernet LAN access is required. To open the interface:

1. Connect the Ethernet patch cable (supplied with the product) to the RJ-45 connector (labelled **10/100**) at the front panel.
2. Connect the remaining end of the Ethernet cable to the Internet or LAN segment as directed by the customer.
3. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
4. Enter the default Internet Protocol (IP) address of the switch (**10.1.1.10**) as the uniform resource locator (URL). The *Enter Network Password* dialog box displays.
5. Type the case-sensitive default user name (**Administrator**) and password (**password**) and click *OK*. The *First Time Login View* displays.
6. Type customer-specified values in the *User Name*, *New Password*, and *Confirm Password* fields, then click *Activate*. The *Topology View* displays with status information about each fabric element, including the product to be configured.
7. Click *Switch Details*. The *Hardware View* displays (Figure 2-1).
8. To configure the product from the EFCM Basic Edition interface, selectively perform the following tasks according to customer requirements:
  - **Product** - includes identification, date and time, parameters, fabric parameters, and network addresses.
  - **Ports** - includes basic information, buffer-to-buffer credits (BB\_Credits), and N\_Port identifier virtualization (NPIV).
  - **Management** - includes SNMP trap message recipients, command line interface (CLI), open systems management server (OSMS), secure socket layer (SSL) encryption.
  - **Options** - includes product feature enablement (PFE) keys.
  - **Interswitch links** - includes preferred path and interswitch link (ISL) port fencing.



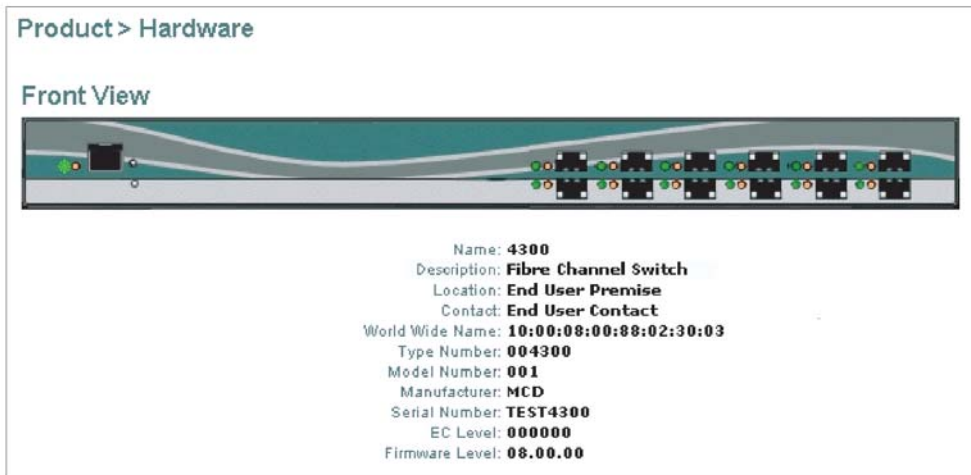


Figure 2-1 Hardware View

## Configure Product Identification

Perform this procedure to configure the product identification. The *Name*, *Location*, and *Contact* variables correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*, and are used by management workstations when obtaining product data.

1. Select *Switch* and *Identification* from the *Configure* menu at any view. The *Identification View* displays (Figure 2-2).

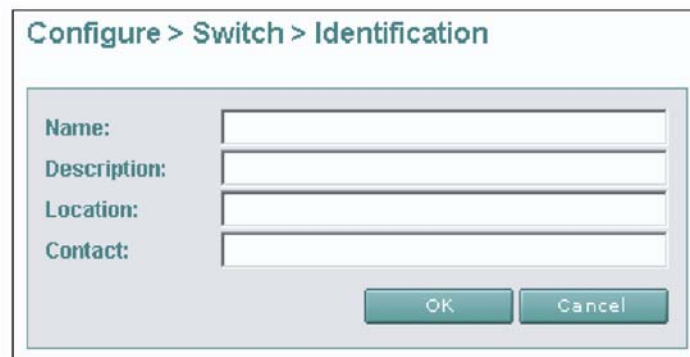


Figure 2-2 Identification View

- a. Type a unique product name of 24 alphanumeric characters or less in the *Name* field. If installed on a public LAN, the name should reflect the product's Ethernet network domain name system (DNS) host name.
  - b. Type a product description of 255 alphanumeric characters or less in the *Description* field.
  - c. Type the product's physical location (255 alphanumeric characters or less) in the *Location* field.
  - d. Type the name of a contact person (255 alphanumeric characters or less) in the *Contact* field.
2. Click *OK* to save and activate changes.

## Configure Date and Time

Perform this procedure to configure product date and time.

1. Select *Switch* and *Date & Time* from the *Configure* menu at any view. The *Date Time View* displays (Figure 2-3).

124M1130

Figure 2-3 Date Time View

- a. Click *Date* fields that require change, and type numbers in the following ranges:
  - Month (*MM*): 1 through 12.
  - Day (*DD*): 1 through 31.
  - Year (*YYYY*): greater than 1980.

- b. Click *Time* fields that require change, and type numbers in the following ranges:
  - Hour (*HH*): **0** through **23**.
  - Minute (*MM*): **0** through **59**.
  - Second (*SS*): **0** through **59**.
2. Click *OK* to save and activate changes.

## Configure Parameters

Perform this procedure to configure product operating parameters.

1. Set the product offline. Refer to [Set Online State](#) for instructions.
2. Select *Switch* and *Parameters* from the *Configure* menu at any view. The *Parameters View* displays ([Figure 2-4](#)).
  - a. At the *Insistent Domain ID* field, check (enable) or uncheck (disable) the parameter. When enabled, the value configured in the *Preferred Domain ID* field becomes the active domain ID when the fabric initializes.

The screenshot shows a configuration window titled "Configure > Switch > Parameters". It contains several checkboxes for parameters: "Insistent Domain ID", "Rerouting Delay", "Domain RSCN", "Suppress RSCN on Zone Set Activations", "Limited Fabric RSCN", and "Zone FlexPars: Isolate Fabric RSCNs on zone activation changes". Below these is a text input field for "'Preferred Domain ID" containing the value "1", and a dropdown menu for "'ISL FSPF Cost Configuration:" set to "By Port Speed". A warning message at the bottom states: "'The device must be offline to activate changes to this parameter." At the bottom right are "OK" and "Cancel" buttons.

i24M1134

Figure 2-4 Parameters View

- b. At the *Rerouting Delay* field, check (enable) or uncheck (disable) the parameter. When enabled, traffic is delayed through the fabric by the user-specified error detect time out value (E\_D\_TOV). This delay ensures Fibre Channel frames are delivered to their destination in order.
- c. At the *Domain RSCN* field, check (enable) or uncheck (disable) the parameter. When enabled, attached devices can register to receive notification when other devices change state.
- d. At the *Suppress RSCN on Zone Set Activations* field, check (enable) or uncheck (disable) the parameter. When enabled, RSCNs are not transmitted when a zone set is activated.
- e. At the *Limited Fabric RSCN* field, check (enable) or uncheck (disable) the parameter. When enabled, RSCNs are not transmitted after a product initial program load (IPL).
- f. At the *Zone Flexpars: Isolate Fabric RSCNs on zone activation changes* field, check (enable) or uncheck (disable) the parameter. When enabled, zone FlexPars isolate and prevent fabric-format RSCNs from propagating to devices in zones that are not impacted.
- g. At the *Preferred Domain ID* field, type a value between **1** through **31**. This value uniquely identifies each fabric element.

---

**NOTE:** An ISL between fabric elements with identical domain IDs segments and prevents communication.

---

- h. At the *ISL FSPF Cost Configuration* field, select *By Port Speed* or *Ignore Port Speed* to calculate fabric shortest path first (FSPF) cost.
    - **By Port Speed** - The fastest fabric path is determined by port (ISL) speed. Cost is inversely proportional to speed.
    - **Ignore Port Speed** - ISL speed is ignored, and the fastest fabric path is determined by the number of hops. Cost is directly proportional to hop count.
3. Click *OK* to save and activate changes.
  4. Set the product online. Refer to [Set Online State](#) for instructions.

## Configure Fabric Parameters

Perform this procedure to configure fabric operating parameters.

1. Set the product offline. Refer to [Set Online State](#) for instructions.
2. Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays (Figure 2-5).

Figure 2-5 Fabric Parameters View

- a. At the *R\_A\_TOV* field, type a value between **10** through **1200** tenths of a second (one through 120 seconds). Ten seconds (**100**) is the recommended value. The *R\_A\_TOV* value must exceed the *E\_D\_TOV* value.
- b. At the *E\_D\_TOV* field, type a value between **2** through **600** tenths of a second (0.2 through 60 seconds). Two seconds (**20**) is the recommended value.

---

**NOTE:** Fabric elements must be set to the same *R\_A\_TOV* and *E\_D\_TOV* values. An ISL between fabric elements with different values segments and prevents communication.

---

- c. Select from the *Switch Priority* drop-down list to designate the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself). Available selections are *Default*, *Principal*, and *Never Principal*.

*Principal* is the highest priority setting, *Default* is next, and *Never Principal* is the lowest. At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment.

- d. Select from the *Interop Mode* drop-down list to set the product operating mode. This setting affects the management mode and does not affect port operation. Available selections are:
  - **McDATA Fabric 1.0** - Select this option if the product is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.
  - **Open Fabric 1.0** - Select this option (default) for managing heterogeneous fabrics and if the product is fabric-attached to McDATA directors or switches and other open-fabric compliant switches.

---

**NOTE:** With Open Fabric 1.0 enabled, the default zone set is disabled.

---

3. Click *OK* to save and activate changes.
4. Set the product online. Refer to [Set Online State](#) for instructions.

---

## Configure Network Information

Verify the LAN installation with the network administrator. If:

- One product is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change.
- Multiple products are installed or a public LAN segment is used, network information must be changed to conform to the LAN addressing scheme.

Perform this procedure to change product network information.

1. Select *Switch* and *Network* from the *Configure* menu at any view. The *Network View* displays ([Figure 2-6](#)).
  - a. At the *IP Address* field, type the new value as specified by the network administrator (default is **10.1.1.10**).
  - b. At the *Subnet Mask* field, type the new value as specified by the network administrator (default is **255.0.0.0**).
  - c. At the *Gateway Address* field, type the new value as specified by the network administrator (default is **0.0.0.0**).

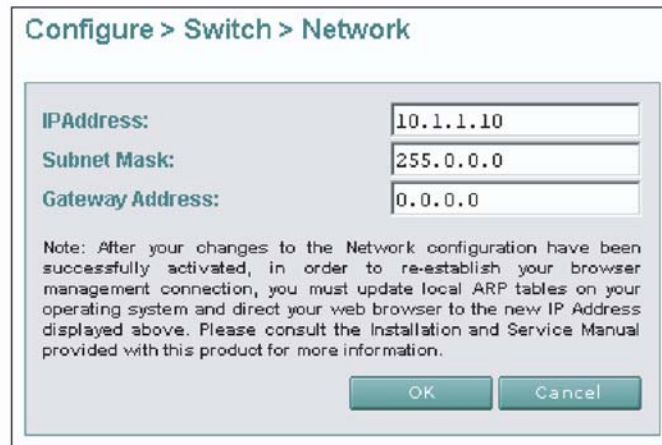


Figure 2-6 Network View

2. Click *OK* to save and activate changes. An acknowledgement message displays, indicating the browser PC must be directed to the new IP address.
3. Update the address resolution protocol (ARP) table for the browser PC.
  - a. Close the EFCM Basic Edition interface and all browser applications.
  - b. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.
  - c. At the *Windows Workstation* menu, sequentially select the *Programs* and *Command Prompt* options. A disk operating system (DOS) window displays.
  - d. Delete the switch's *old* IP address from the ARP table. At the command (C:\) prompt, type **arp -d xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the old IP address for the switch.
  - e. Click close (*X*) at the upper right corner of the DOS window to close the window and return to the Windows desktop.
4. At the product front panel, press and hold the **IML/RESET** button for ten seconds to perform a power-on reset (POR).

5. At the PC, launch the browser application (Netscape Navigator or Internet Explorer). Enter the product's **new** IP address as the Internet URL. The *Enter Network Password* dialog box displays.
6. Type the case-sensitive user name and password and click *OK*. The EFCM Basic Edition interface opens and the *Topology View* displays with status information about each fabric element.

## Configure Basic Port Information

Perform this procedure to configure basic port information.

1. Select *Ports* and *Basic Info* from the *Configure* menu at any view. The *Basic Information View* displays (Figure 2-7).

The screenshot shows a web-based configuration interface titled "Configure > Ports > Basic Information". At the top, there is a "Jump to Port:" field with the value "0" and a "go" button. Below this is a table with the following columns: "Port", "Name", "Blocked", "FAN", "Type", and "Speed". The table contains 11 rows, numbered 0 through 10. Each row has a "Name" field, a "Blocked" checkbox (all are unchecked), a "FAN" checkbox (all are checked), a "Type" dropdown menu, and a "Speed" dropdown menu. The "Type" dropdowns show "Gx Port" for ports 0-3, 5-10 and "F Port" for ports 4 and 6. The "Speed" dropdowns show "Negotiate" for ports 0-3, 5-10 and "1 G" for ports 4 and 6. At the bottom right of the window are "OK" and "Cancel" buttons.

Port	Name	Blocked	FAN	Type	Speed
0		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
1		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
2		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
3		<input type="checkbox"/>	<input checked="" type="checkbox"/>	F Port	1 G
4		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
5		<input type="checkbox"/>	<input checked="" type="checkbox"/>	F Port	1 G
6		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
7		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
8		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
9		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
10		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate

Figure 2-7 Basic Information View

- a. For each port to be configured, type a port name of 24 alphanumeric characters or less in the *Name* field. The port name should characterize the device to which the port is attached.
- b. Click a check box in the *Blocked* column to block or unblock a port (default is unblocked). A check mark indicates a port is blocked.



- c. Click the check box in the *FAN* column to enable or disable the fabric address notification (FAN) feature (default is enabled). A check mark indicates FAN is enabled. When enabled, an *FL\_Port* transmits FAN frames after loop initialization to verify FC-AL devices are still logged in.
  - d. Select from the drop-down list in the *Type* column to configure the port type. Available selections are fabric port (**F\_Port**), expansion port (**E\_Port**), generic port (**G\_Port**), generic mixed port (**GX\_Port**), and fabric mixed port (**FX\_Port**).
  - e. Select from the drop-down list in the *Speed* column to configure the port transmission rate. Available selections are auto-negotiate between speeds (**Negotiate**), 1.0625 gigabit per second (Gbps) operation (**1 Gb/sec**), and 2.1250 Gbps operation (**2 Gb/sec**).
2. Click *OK* to save and activate changes.

---

## Configure Port BB\_Credit

With the full-fabric PFE key enabled, the switch provides a port buffer pool of 144 receive BB\_Credits. Each port can be assigned between two and 12 credits, provided the total credits allocated to all ports does not exceed 144. The default value is five credits per port or 12 credits per port with the full-fabric PFE key enabled. Perform this procedure to configure port receive BB\_Credit:

1. Set all or a subset of user-specified ports offline. Refer to [Set Online State](#) or [Block or Unblock a Port](#) for instructions.
2. Select *Ports* and *RX BB\_Credit* from the *Configure* menu at any view. The *RX BB\_Credit View* displays.
3. Perform one of the following:
  - To set all offline ports to default values, click *Default*.
  - To set an offline port to a user-specified value, type the desired value in the *RX BB\_Credit* column.
4. Click *OK* to save and activate changes.
5. Set all or user-specified ports online. Refer to [Set Online State](#) (all) or [Block or Unblock a Port](#) (specified ports) for instructions.

## Configure Port NPIV

NPIV allows multiple (up to 256) Fibre Channel addresses to be assigned to a node (N\_Port). The NPIV feature must be installed. Refer to [Install PFE Keys \(Optional\)](#) for instructions. Perform this procedure to configure ports for NPIV connectivity.

1. Select *Ports* and *NPIV* from the *Configure* menu at any view. The *NPIV View* displays.
2. Click *Enable* to activate product NPIV operation.
3. To set a port to a user-specified value, type the desired value (1 through 256) in the *Login* column.
4. Click *OK* to save and activate changes.

## Configure SNMP

Perform this procedure to configure names, write authorizations, addresses, and user datagram protocol (UDP) port numbers for SNMP trap message recipients. To configure recipient workstations:

1. Select *SNMP* from the *Configure* menu at any view. The *SNMP View* displays ([Figure 2-8](#)).

Configure > SNMP

SNMP Agent: Enabled

FA MIB Version: FA MIB 3.1

Enable Authentication Traps

Name	Write Auth	Trap Recipient	UDP Port
public	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

i24M1143

Figure 2-8 SNMP View

- a. Click *Enable* to activate the installed SNMP agent.
  - b. Select the appropriate Fibre Alliance management information base (FA MIB) from the *FA MIB Version* drop-down list. Valid selections are **FA MIB Version 3.0** or **FA MIB Version 3.1**.
  - c. Click (check) the *Enable Authentication Traps* check box to enable transmission of SNMP trap messages to recipients.
  - d. For each configured recipient, type a community name of 32 alphanumeric characters or less in the *Name* field. The name is incorporated in SNMP trap messages to ensure against unauthorized viewing.
  - e. Click (check) the box in the *Write Auth* column to enable write authorization for the trap recipient (default is disabled). When enabled, a configured user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.
  - f. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field. It is recommended the IP address be used.
  - g. Type a decimal port number in the *UDP Port Number* field to specify the UDP port number
2. Click *OK* to save and activate changes.

---

## Enable CLI

Perform this procedure to toggle (enable or disable) the state of the product's command line interface. To change the CLI state:

1. Select *CLI* from the *Configure* menu at any view. The *CLI View* displays (Figure 2-9).
2. Perform one of the following:
  - Click *Enable* to activate the CLI.
  - Click *Disable* to deactivate the CLI.
3. Click (check) the *Use SSH* check box to enable secure shell (SSH) protocol. The protocol controls CLI access to the product and provides software-enforced encryption.
4. Click *OK* to save and activate changes.



i24M1137

Figure 2-9 CLI View

## Enable or Disable Host Control

Perform this procedure to configure the open systems management server and enable OSI host control of the product. Implementing and enabling OSI host control requires installation of a SAN management application on the OSI server. Applications include Veritas® SANPoint™ Control or Tivoli® NetView®. To enable or disable OSMS host control:



1. Select *OSMS* from the *Configure* menu at any view. The *OSMS View* displays (Figure 2-10).



i24M1138

Figure 2-10 OSMS View

2. Perform one of the following:
  - Click *Enable* to activate OSMS.
  - Click *Disable* to deactivate OSMS.

3. Click (check) the *Enable Host Control* check box to activate host control of the product.
4. Click *OK* to save and activate changes.

## Configure SSL Encryption

SSL is a protocol that encrypts internet communications. The protocol uses key encryption and includes a digital certificate that enables server authentication and SSL session initialization. To configure SSL encryption:

1. Select *SSL* from the *Configure* menu at any view. The *SSL View* displays (Figure 2-11).

Configure > SSL

Web SSL: Disabled

Software SSL: Disabled

**Current Certificate Details**

Certificate:  
The certificate is set to the factory default (not generated).

MD5:  
The fingerprint is not available (no certificate).

SHA-1:  
The fingerprint is not available (no certificate).

**New Certificate**

Expires in  Days

**SSL Renegotiation**

Renegotiate after  MB

i24M1144

Figure 2-11 SSL View

2. With web SSL enabled, all data transmitted over an authenticated Internet connection is encrypted. Perform one of the following:
  - Click *Enable* to activate web SSL.
  - Click *Disable* to deactivate web SSL.

3. Software SSL enables use of an application program interface (API) connection. With software SSL enabled, secure and unsecure communications are acceptable, however, unsecure communications are directed to an encrypted API connection. Perform one of the following:
  - Click *Enable* to activate software SSL.
  - Click *Disable* to deactivate software SSL.
4. To define the expiration period (in days) of the digital certificate, type a value between **30** and **3650** in the *Expires in* field. The default is **365** days. Click *Generate* to generate a new certificate.
5. To define a renegotiation parameter (in megabytes) for the SSL session key, type a value between **50** and **10000** in the *Renegotiate after* field. The value defines the MB of data transmitted over the connection before triggering the regeneration of a new SSL session key. An SSL session key (not part of the digital certificate) is valid only during the SSL connection, and is renegotiated per the value entered.
6. Click *OK* to save and activate changes.

---

### Install PFE Keys (Optional)

The following PFE-keyed options are available:

- **Flexport Technology** - A Flexport Technology product is delivered at a discount without all Fibre Channel ports enabled. When additional port capacity is required, the remaining ports are incrementally enabled through this feature.
- **Full-fabric capability** - This feature allows Fibre Channel ports to be configured as E\_Ports, G\_Ports, or GX\_ports, and supports additional port BB\_Credits.
- **Full volatility** - This feature ensures no Fibre Channel frames are stored after the product is powered off or fails, and a memory dump file (that possibly includes classified data frames) is not included as part of the data collection procedure.

After purchasing a feature, obtain the PFE key by following the enclosed instructions. The key is an alphanumeric string consisting of uppercase and lowercase characters that must be entered exactly, including dashes. An example format is:

**XxXx-XXxX-xxXX-xX.**

Keys are encoded to work only with the serial number of the installed product. Record the key to re-install the feature if required. If the product fails and is replaced, obtain new PFE keys from the solution center (**800-752-4572** or **support@mcddata.com**). Have the serial numbers of the failed and replacement products, and the old PFE key number or transaction code. After obtaining a PFE key, install the feature as follows:

1. Select *Upgrade Options* from the *Configure*, *Maintenance*, or *Security* menus at any view. The *Maintenance Feature Installation View* displays (Figure 2-12).

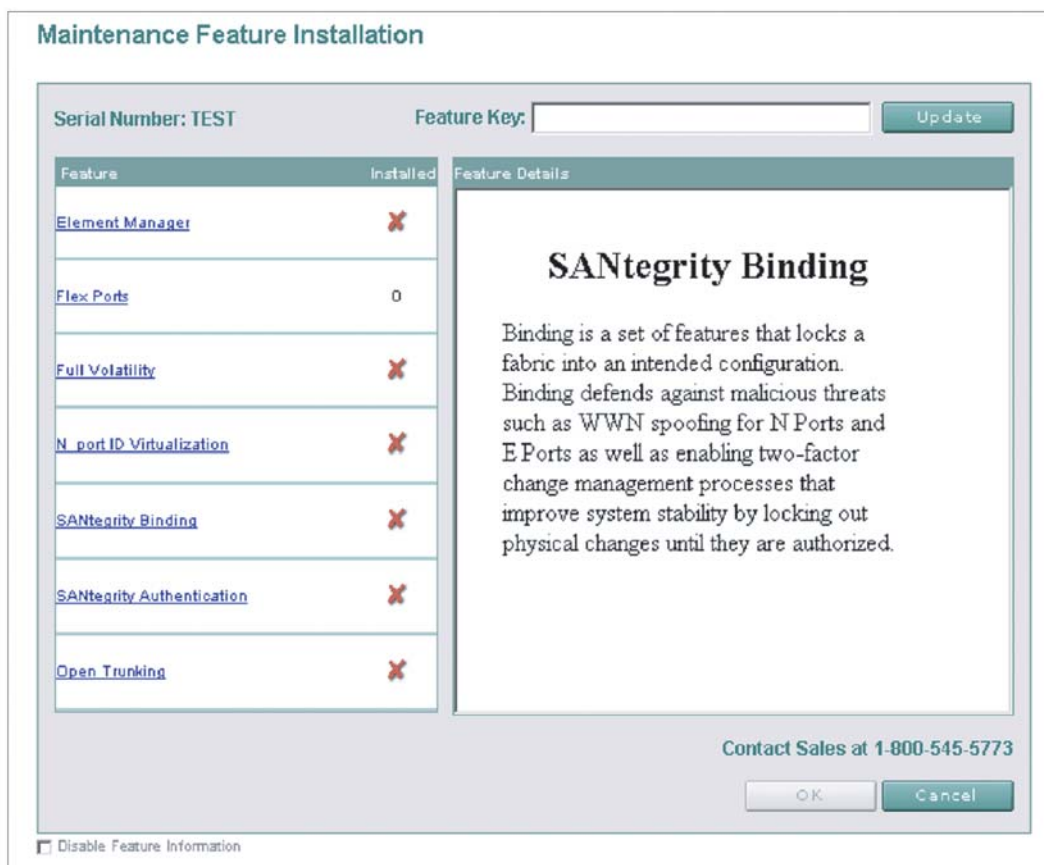


Figure 2-12 Maintenance Feature Installation View

Feature status is indicated by a green check mark ✓ (installed) or a red X (uninstalled). Flexport Technology status is indicated by the number of installed ports. Click a feature title in the *Feature* panel and a description appears in the *Feature Details* panel.

2. Type the key in the *Feature Key* field and click *Update*. The interface refreshes and indicates the update changes in the *Feature* panel.

---

**NOTE:** When *OK* is selected, all features are updated with new features.

---

3. Click *OK*. New PFE key(s) activate, the message **Feature installation in process. Your browser connection will be unavailable until unit restart is complete.** displays, and the product performs a non-disruptive (to Fibre Channel traffic) firmware reset.
4. After the product reset, the message **Feature installation complete. Click [here](#) to login.** displays.
5. Click [here](#) to login and start a new EFCM Basic Edition session. The *Enter Network Password* dialog box displays.

---

## Configure Interswitch Links

This section describes optional ISL performance features configured through *Configure* menu selections. Features include:

- **Preferred path** - Use the *Preferred Path View* to specify and configure one or more ISL data paths between multiple fabric elements. At each fabric element, a preferred path consists of a source port, exit port, and destination Domain\_ID.
- **Port fencing** - Use the *Port Fencing View* to minimize ISLs that bounce (repeatedly attempt to establish a connection), causing disruptive fabric rebuilds. Fencing defines a bounce threshold that when reached, automatically blocks the disruptive E\_Port.

To configure optional features, refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

Verify the LAN installation with the customer. If multiple products are installed or a public LAN segment is used, network addresses must be changed to conform to the customer's LAN addressing scheme. Go to [Task 4: Configure Product Network Information \(Optional\)](#).

If no additional options, features, or network addresses are to be configured, go to [Task 5: Cable Fibre Channel Ports](#).



## Task 4: Configure Product Network Information (Optional)

The product is delivered with default network addresses as follows:

- **MAC address** - The media access control (MAC) address is programmed into FLASH memory on the control processor (CTP) card at manufacture. The MAC address is unique for each product, and should not be changed.
- **IP address** - The default IP address is **10.1.1.10**. If multiple products are installed on the same LAN, each product (and the management server) must have a unique IP address.

---

**NOTE:** If multiple products and the management server are delivered in a Fabriccenter equipment cabinet, all devices are configured with unique IP addresses that do not require change. The addresses require change only if multiple cabinets are LAN-connected.

---

- **Subnet mask** - The default subnet mask is **255.0.0.0**. If the product is installed on a complex public LAN with one or more routers, the address may require change.
- **Gateway address** - The default gateway address is **0.0.0.0**. If the product is installed on a public LAN, the gateway address must be changed to the address of the corporate intranet's local router.

Perform the following steps to change a product IP address, subnet mask, or gateway address. An asynchronous RS-232 modem cable and maintenance terminal (desktop or notebook PC) with a Windows-based operating system and RS-232 serial communication software (such as ProComm Plus or HyperTerminal) are required.

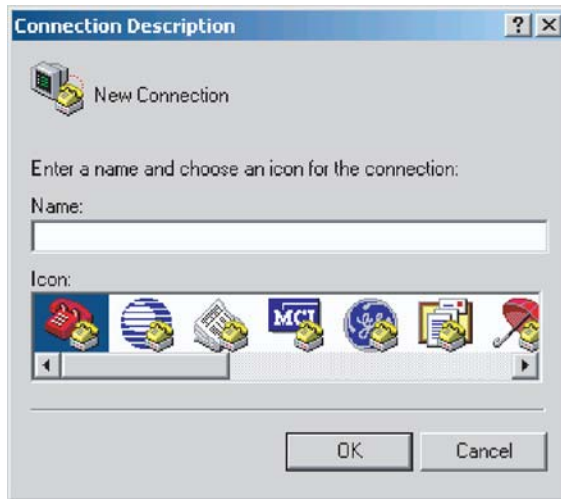
1. Using a Phillips screwdriver, remove the protective cap from the 9-pin maintenance port at the rear of the chassis. Connect one end of the RS-232 modem cable to the port.
2. Connect the other cable end to a 9-pin serial communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

---

**NOTE:** The following steps describe changing network addresses using HyperTerminal serial communication software.

---

4. At the *Windows Workstation* menu, sequentially select the *Programs*, *Accessories*, *Communications*, and *HyperTerminal* options. The *Connection Description* dialog box displays (Figure 2-13).



i24M1158

Figure 2-13 Connection Description Dialog Box

5. Type a descriptive product name in the *Name* field and click *OK*. The *Connect To* dialog box displays.
6. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the port connection to the product), and click *OK*. The *COMn Properties* dialog box displays, where *n* is **1** or **2**.
7. Configure *Port Settings* parameters:
  - *Bits per second* - **115200**.
  - *Data bits* - **8**.
  - *Parity* - **None**.
  - *Stop bits* - **1**.
  - *Flow control* - **Hardware** or **None**.
 Click *OK*. The *New Connection - HyperTerminal* window displays.

8. At the > prompt, type the user password (default is **password**) and press **Enter**. The password is case sensitive. The *New Connection - HyperTerminal* window displays with software and hardware version information for the product, and a **C >** prompt at the bottom of the window.
9. At the **C >** prompt, type the **ipconfig** command and press **Enter**. The *New Connection - HyperTerminal* window displays with configuration information listed:
  - *MAC Address.*
  - *IP Address* (default is **10.1.1.10**).
  - *Subnet Mask* (default is **255.0.0.0**).
  - *Gateway Address* (default is **0.0.0.0**).
  - *Auto Negotiate.*
  - *Speed.*
  - *Duplex.*

Only the *IP Address*, *Subnet Mask*, and *Gateway Address* fields are configurable.

10. Change the IP address, subnet mask, and gateway address as directed by the customer. To change the addresses, type the following at the **C >** prompt and press **Enter**.

```
ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz
```

The IP address is **xxx.xxx.xxx.xxx**, the subnet mask is **yyy.yyy.yyy.yyy**, and the gateway address is **zzz.zzz.zzz.zzz**, where the octets **xxx**, **yyy**, and **zzz** are decimals from zero through 255. If an address is to remain unchanged, type the current address in the respective field.

11. Select *Exit* from the *File* pull-down menu. A HyperTerminal message box appears.
12. Click *Yes*. A second message box appears. Click *No* to exit and close the application.
13. Power off the maintenance terminal and disconnect the RS-232 modem cable. Replace the protective cap over the maintenance port.
14. At the product front panel, press and hold the **IML/RESET** button for ten seconds to perform a POR.

15. Connect the product to the customer-supplied Ethernet LAN segment:
  - a. Connect one end of the Ethernet patch cable (supplied) to the RJ-45 connector (labelled **10/100**).
  - b. Connect the remaining end of the cable to the LAN as directed by the customer.

---

## Task 5: Cable Fibre Channel Ports

Perform this task to cable Fibre Channel ports and connect devices:

1. Route fiber-optic jumper cables from customer-specified Fibre Channel devices, FC-AL devices, or fabric elements to product ports.
2. Connect device cables to SFP optical port transceivers as directed by the customer.
3. Perform one of the following:
  - If the product is installed on a table or desktop, bundle and secure Fibre Channel cables as directed by the customer.
  - If the product is installed in a customer-supplied equipment rack, bundle Fibre Channel cables from the product and other equipment (groups of 16 maximum), and secure them as directed by the customer.
  - If the product is installed in a Fabriccenter equipment cabinet, bundle Fibre Channel cables from the product and other equipment (groups of 16 maximum), and secure them in the cable management area at the front-left side of the cabinet.

---

## Task 6: Configure Zoning (Optional)

Perform this procedure to configure, change, add, or delete zones; and to configure, change, enable, or disable zone sets.

- **Zone** - A zone is a group of devices that can access each other through port-to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.

- **Zone set** - A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time.

The following naming conventions apply to zones and zone sets:

- All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
- The first character of a zone set name must be a letter (**A** through **Z** or **a** through **z**).
- A zone set name cannot contain spaces.
- Valid characters are alphanumeric and the caret ( **^** ), hyphen ( **-** ), underscore ( **\_** ), or dollar ( **\$** ) symbols.
- A zone set name can have a maximum of 64 characters.

To configure zones and zone sets, refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

---

## Task 7: Connect Product to a Fabric Element (Optional)

To provide fabric-attached Fibre channel connectivity for devices connected to the product, connect the product to an expansion port (E\_Port) of a fabric element (switch or director). Any switch can be used to form this ISL. To connect the product to a fabric element and create an ISL:

1. Ensure the fabric element is accessible by the EFCM Basic Edition interface. If the fabric element must be defined, refer to the appropriate switch or director installation manual for instructions.
2. Ensure the preferred domain ID for the product is unique and does not conflict with the ID of another switch or director participating in the fabric. Refer to [Task 3: Configure Product at the EFCM Basic Edition Interface](#).
3. Ensure R\_A\_TOV and E\_D\_TOV values for the product are identical to the values for all switches or directors participating in the fabric. Refer to [Task 3: Configure Product at the EFCM Basic Edition Interface](#).

4. Route a multimode or singlemode fiber-optic cable (depending on the type of transceiver installed) from a customer-specified E\_Port of the fabric element to the front of the product.
5. Connect the fiber-optic cable to a product port as directed by the customer.
6. Select *Port List* from the *Product* menu at any view. The *Port List View* displays.
7. At the *Port List View*, click the physical port number of the fabric ISL (connected in [step 5](#)) in the *Port* column. Physical properties for the port appear in the lower panel of the view.
8. Ensure the *Operational State* field displays **Online** and the *Reason* field displays N/A or is blank. If an ISL segmentation or other problem is indicated, go to [MAP 0000: Start MAP](#) to isolate the problem. If no problems are indicated, installation tasks are complete.

---

## Task 8: Register with the McDATA File Center

To complete the installation, register with the McDATA Filecenter web site to receive e-mail updates and access the following:

- Technical publications.
- Firmware and software upgrades.
- Technical newsletters.
- Release notes.

To register with the Filecenter:

1. At the server with Internet access, open the McDATA home page (<http://mcddata.com>). Select *File Center* from the *Support* menu. The Filecenter home page opens ([Figure 2-14](#)).
2. Select (click) the *New User Registration* option at the top of the home page. The Filecenter's *New User Registration* page displays. Use the page to input user information. The following is required:
  - Password.
  - Verify password.
  - First, middle, and last name.
  - E-mail address.

- Company.
- Title.
- Telephone and facsimile numbers.



Figure 2-14 McDATA Filecenter Home Page

3. Complete fields as required and click *Register*. The registration is complete and Filecenter login information is transmitted to the e-mail address specified.
4. At the browser PC, close the Internet session. If no product problems are indicated, installation tasks are complete.





This chapter describes maintenance analysis procedures (MAPs) used by service representatives to fault isolate Sphereon 4300 Fabric Switch problems or failures to the field-replaceable unit (FRU) level. MAPs consist of step-by-step procedures that provide information to interpret system events, isolate a failure to a single FRU, remove and replace the failed FRU, and verify product operation.

## Factory Defaults

[Table 3-1](#) lists factory defaults for product passwords (customer and maintenance level), and the product's Internet Protocol (IP) address, subnet mask, and gateway address.

Table 3-1 Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

## Quick Start

[Table 3-2](#) lists and summarizes MAPs. Fault isolation normally begins at [MAP 0000: Start MAP](#).

Table 3-2 MAP Summary

MAP	Page
MAP 0000: Start MAP	<a href="#">3-5</a>
MAP 0100: Power Distribution Analysis	<a href="#">3-9</a>
MAP 0200: POST Failure Analysis	<a href="#">3-10</a>
MAP 0300: Loss of Browser PC Communication	<a href="#">3-11</a>
MAP 0400: FRU Failure Analysis	<a href="#">3-14</a>
MAP 0500: Port Failure or Link Incident Analysis	<a href="#">3-16</a>
MAP 0600: Fabric or ISL Problem Analysis	<a href="#">3-27</a>

[Table 3-3](#) lists event codes, corresponding MAP references, and provides a quick start guide if an event code is readily available.

Table 3-3 Event Codes versus Maintenance Action

Event Code	Explanation	Action
011	Login Server database invalid.	Go to <a href="#">MAP 0600</a> .
021	Name Server database invalid.	Go to <a href="#">MAP 0600</a> .
031	SNMP request received from unauthorized community.	Add a community name.
051	Management Server database invalid.	Go to <a href="#">MAP 0600</a> .
061	Fabric Controller database invalid.	Go to <a href="#">MAP 0600</a> .
062	Maximum interswitch hop count exceeded.	Go to <a href="#">MAP 0600</a> .
063	Remote switch has too many ISLs.	Go to <a href="#">MAP 0600</a> .
064	ESS response from indicated domain ID not received after maximum tries.	No action required.
070	E_Port is segmented.	Go to <a href="#">MAP 0600</a> .

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
071	Switch is isolated.	Go to <a href="#">MAP 0600</a> .
072	E_Port connected to unsupported switch.	Go to <a href="#">MAP 0600</a> .
073	Fabric initialization error.	Go to <a href="#">Collect Maintenance Data</a> .
074	ILS frame delivery error threshold exceeded.	Go to <a href="#">Collect Maintenance Data</a> .
075	E_Port segmentation recovery.	No action required.
080	Unauthorized worldwide name.	Go to <a href="#">MAP 0500</a> .
081	Invalid attachment.	Go to <a href="#">MAP 0500</a> .
082	Port fenced.	Go to <a href="#">MAP 0600</a> .
083	Port set to inactive state.	Go to <a href="#">MAP 0500</a> .
120	Error detected while processing system management command.	Go to <a href="#">Collect Maintenance Data</a> .
121	Zone set activation failed - zone set too large.	Reduce size of zone set and retry.
140	Congestion detected on an ISL.	Go to <a href="#">MAP 0600</a> .
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to <a href="#">MAP 0600</a> .
143	Low BB_Credit relieved on an ISL.	No action required.
150	Fabric merge failure.	Go to <a href="#">MAP 0600</a> .
151	Fabric configuration failure.	Go to <a href="#">Collect Maintenance Data</a> .
300	Cooling fan propeller failed.	Go to <a href="#">MAP 0400</a> .
301	Cooling fan propeller failed.	Go to <a href="#">MAP 0400</a> .
302	Cooling fan propeller failed.	Go to <a href="#">MAP 0400</a> .
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
370	Cooling fan status polling temporarily disabled.	Go to <a href="#">MAP 0400</a> .
400	Power-up diagnostic failure.	Go to <a href="#">MAP 0200</a> .

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
410	Switch reset.	No action required.
411	Firmware fault.	Go to <a href="#">MAP 0200</a> .
412	CTP watchdog timer reset.	Go to <a href="#">Collect Maintenance Data</a> .
421	Firmware download complete.	No action required.
423	CTP firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	Go to <a href="#">MAP 0400</a> .
433	Non-recoverable Ethernet fault.	Go to <a href="#">MAP 0400</a> .
440	Embedded port hardware failed.	Go to <a href="#">MAP 0400</a> .
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
453	New feature key installed.	No action required.
506	Fibre Channel port failure.	Go to <a href="#">MAP 0500</a> .
507	Loopback diagnostics port failure.	Go to <a href="#">MAP 0500</a> .
508	Fibre Channel port anomaly detected.	No action required.
510	Optical transceiver hot-insertion initiated.	No action required.
512	Optical transceiver nonfatal error.	Go to <a href="#">MAP 0500</a> .
513	Optical transceiver hot-removal completed.	No action required.
514	Optical transceiver failure.	Go to <a href="#">MAP 0500</a> .
515	Optical digital diagnostics warning threshold exceeded.	Go to <a href="#">MAP 0500</a> .
516	Optical digital diagnostics alarm threshold exceeded.	Go to <a href="#">MAP 0500</a> .
523	FL_Port open request failed.	No action required.
524	No AL_PA acquired.	No action required.
525	FL_Port arbitration timeout.	No action required.
581	Implicit incident.	Go to <a href="#">MAP 0500</a> .
582	Bit error threshold exceeded.	Go to <a href="#">MAP 0500</a> .

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
583	Loss of signal or loss of synchronization.	Go to <a href="#">MAP 0500</a> .
584	Not operational primitive sequence received.	Go to <a href="#">MAP 0500</a> .
585	Primitive sequence timeout.	Go to <a href="#">MAP 0500</a> .
586	Invalid primitive sequence received for current link state.	Go to <a href="#">MAP 0500</a> .
810	High temperature warning (CTP thermal sensor).	Go to <a href="#">MAP 0400</a> .
811	Critically hot temperature warning (CTP thermal sensor).	Go to <a href="#">MAP 0400</a> .
812	CTP card shutdown due to thermal violations.	Go to <a href="#">MAP 0400</a> .
850	Switch shutdown due to CTP thermal violations.	Go to <a href="#">MAP 0400</a> .

## MAP 0000: Start MAP

This MAP describes initial fault isolation beginning at the:

- Failed product.
- Browser-capable PC with Internet connectivity to the firmware-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface.
- Product-attached open systems interconnection (OSI) host console.

### 1

Prior to fault isolation, acquire:

- A system configuration drawing or planning worksheet that includes the location of the product, management interface, other McDATA products, and device connections.
- The internet protocol (IP) address, gateway address, and subnet mask for the product reporting the problem.
- User IDs and passwords.

**Continue to the next step.**

## 2

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is the product powered on?

**YES NO**

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#). **Exit MAP.**

## 3

At the failed product, inspect the amber **ERR** LED and amber LEDs associated Fibre Channel ports and FRUs.

Are any amber LEDs illuminated?

**NO YES**

- ↓ A FRU failure, power-on self-test (POST) failure, link incident, interswitch link (ISL) problem, fenced E\_Port, or segmented E\_Port is indicated. To obtain event codes that identify the failure, **go to step 10.**

## 4

Is the product management interface (browser PC or OSI host console) powered on and operational?

**NO YES**

- ↓ **Go to step 7.**

## 5

Power on the management interface platform and launch the associated management application:

- **EFCM Basic Edition** - Refer to [Task 3: Configure Product at the EFCM Basic Edition Interface](#) for instructions.
- **OSI host console** - Refer to documentation supplied with the host system for instructions.

Was the maintenance action successful?

**NO YES**

↓ Go to [step 7](#).

## 6

Inspect the management interface for communication link failure. Observe a **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or similar message.

Was a failure indication observed?

**NO YES**

↓ Communication with the EFCM Basic Edition interface failed. Go to [MAP 0300: Loss of Browser PC Communication](#). **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

## 7

Inspect product status at the management interface:

- a. For the product reporting the problem:
  - **EFCM Basic Edition** - Select *Hardware* from the *Product* menu at any view. The *Hardware View* displays.
  - **OSI host console** - **Go to [step 9](#)**.
- b. Inspect the status symbol associated with the product. A yellow triangle (attention indicator) indicates the product is operating in degraded mode. A red diamond (failure indicator) indicates the product is not operational.
- c. Inspect simulated Fibre Channel ports for a yellow triangle (attention indicator) that overlays the FRU graphic.
- d. Inspect simulated FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Is a failure indicated?

**NO YES**

↓ A FRU failure, power-on self-test (POST) failure, link incident, interswitch link (ISL) problem, fenced E\_Port, or segmented E\_Port is indicated. To obtain event codes that identify the failure, **go to [step 10](#)**.

## 8

A link incident may have occurred, but the LIN alerts option is not enabled and the yellow triangle (attention indicator) does not appear. Inspect the *Link Incident Log*:

- a. Select *Link Incident* from the *Logs* menu at any view. The *Link Incident Log* displays.
- b. If a link incident occurred, the port number is listed with one of the following messages.
  - **Link interface incident - implicit incident.**
  - **Link interface incident - bit-error threshold exceeded.**
  - **Link failure - loss of signal or loss of synchronization.**
  - **Link failure - not-operational primitive sequence (NOS) received.**
  - **Link failure - primitive sequence timeout.**
  - **Link failure - invalid primitive sequence received for the current link state.**

Did a listed message appear?

**NO**    **YES**

- ↓ A Fibre Channel link incident is indicated. Go to [MAP 0500: Port Failure or Link Incident Analysis](#). **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

## 9

If an incident occurs on the Fibre Channel link between the product and attached OSI server, a link incident record is generated and sent to the server console using the reporting procedure defined in T11/99-017v0.

Was a link incident record generated and sent to the OSI server?

**NO**    **YES**

- ↓ A Fibre Channel link incident is indicated. Go to [MAP 0500: Port Failure or Link Incident Analysis](#). **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**



## 10

Inspect the *Event Log* to obtain failure reason codes:

- a. Select *Event* from the *Logs* menu at any view. The *Event Log* displays.
- b. Record the event code and associated date, time, and severity (*Informational*, *Minor*, *Major*, or *Severe*).
- c. If multiple event codes are found, record all codes and severity levels. Record the date, time, and sequence, and determine if all codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

Were one or more event codes found?

**NO**    **YES**



**Go to [Table 3-3](#)** to obtain event codes. **Exit MAP.**

**Return to [step 1](#)** and perform fault isolation again. If this is the second time at this step, perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

## MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the product power distribution system, including defective AC power cords or redundant power supplies. The failure indicator is inability of the product to power on.

### 1

Inspect and verify facility power is within specifications:

- One single-phase connection for each power supply.
- Input power between 100 and 240 VAC, at least 5 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

**YES**    **NO**



Ask the customer to correct the facility power problem. When corrected, **continue to the next step.**

## 2

The power supply may be disconnected or failed. Verify connection to facility power.

- a. Ensure the AC power cord is connected to the rear of the switch and a facility power receptacle. If not, connect the power cord as directed by the customer.
- b. Ensure facility circuit breakers are on. If not, ask the customer to set breakers on.
- c. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was the maintenance action successful?

**NO**    **YES**

↓    The product is operational. **Exit MAP.**

A power supply failure is indicated. Replace the switch. **Exit MAP.**

## MAP 0200: POST Failure Analysis

This MAP describes fault isolation for a POST failure. The failure indicator is event code **400** or **411** observed at the *Event Log*.

### 1

[Table 3-4](#) lists event codes, explanations, and MAP steps.

Table 3-4    MAP 200 Event Codes

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to <a href="#">step 2</a> .
411	Firmware fault.	Go to <a href="#">step 3</a> .

### 2

As indicated by event code **400**, POST/IPL diagnostics detected a FRU failure.

- a. At the *Event Log*, examine the first two bytes of event data.

- b. Byte **0** specifies failed FRU. Byte **1** specifies the slot number of the failed FRU (**00** for nonredundant, **00** or **01** for redundant) as listed in [Table 3-5](#).

Table 3-5 MAP 200 Byte 0 FRU Codes

Byte 0	Failed FRU	Action
02	CTP card.	Replace the switch. <b>Exit MAP.</b>
05	Fan module.	Replace the switch. <b>Exit MAP.</b>
06	Power supply.	Replace the switch. <b>Exit MAP.</b>

### 3

As indicated by event code **411**, POST/IPL diagnostics detected a firmware failure and performed an online dump. All Fibre Channel ports reset after failure and devices momentarily logout, login, and resume operation. Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

## MAP 0300: Loss of Browser PC Communication

This MAP describes fault isolation for the product to browser PC Internet connection (EFCM Basic Edition interface). The failure indicator is a **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or similar message.

**NOTE:** Upon restart, it may take up to five minutes for the Internet connection to activate. This delay is normal.

### 1

The browser PC cannot communicate with the product because:

- The product-to-PC Internet link could not be established.
- AC power distribution for the product failed or AC power was disconnected.
- The product CTP card failed.

**Continue to the next step.**

## 2

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is the product powered on?

**YES NO**

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#). **Exit MAP.**

## 3

A product-to-PC link problem (Internet too busy or IP address typed incorrectly) or an Ethernet port failure is indicated.

- a. Wait approximately five minutes, then attempt to login to the product.
- b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the product IP address obtained in [MAP 0000: Start MAP](#). The *Username and Password Required* dialog box appears.
- c. Type the user name and password obtained in [MAP 0000: Start MAP](#) and click *OK*. If the EFCM Basic Edition interface does not open, wait five minutes and perform this step again.

Is the EFCM Basic Edition interface operational?

**NO YES**

- ↓ The Internet connection is restored. **Exit MAP.**

## 4

The IP address defining the product to the interface is incorrect or unknown. An asynchronous RS-232 modem cable and maintenance terminal (desktop or notebook PC) with a Windows-based operating system and RS-232 serial communication software (such as ProComm Plus or HyperTerminal) are required. To determine the IP address:

- a. Using a Phillips screwdriver, remove the protective cap from the 9-pin maintenance port at the rear of the chassis. Connect one end of the RS-232 modem cable to the port.
- b. Connect the other cable end to a 9-pin serial communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
- c. Power on the maintenance terminal. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.
- d. At the *Windows Workstation* menu, sequentially select the *Programs*, *Accessories*, *Communications*, and *HyperTerminal* options. The *Connection Description* dialog box displays.
- e. Type a descriptive product name in the *Name* field and click *OK*. The *Connect To* dialog box displays.
- f. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the port connection to the product), and click *OK*. The *COMn Properties* dialog box displays, where *n* is **1** or **2**.
- g. Configure *Port Settings* parameters:
  - *Bits per second* - **115200**.
  - *Data bits* - **8**.
  - *Parity* - **None**.
  - *Stop bits* - **1**.
  - *Flow control* - **Hardware** or **None**.Click *OK*. The *New Connection - HyperTerminal* window displays.
- h. At the **>** prompt, type the user password (default is **password**) and press **Enter**. The password is case sensitive. The *New Connection - HyperTerminal* window displays with software and hardware version information for the product, and a **C >** prompt at the bottom of the window.
- i. At the **C >** prompt, type the **ipconfig** command and press **Enter**. The *New Connection - HyperTerminal* window displays with configuration information listed.
- j. Record the product IP address.
- k. Select *Exit* from the *File* pull-down menu. A HyperTerminal message box appears.

- l. Click *Yes*. A second message box appears. Click *No* to exit and close the application.
- m. Power off the maintenance terminal and disconnect the modem cable. Replace the protective cap over the maintenance port.

**Continue to the next step.**

## 5

Login to the product using the IP address determined in [step 4](#).

- a. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the new product IP address. The *Username and Password Required* dialog box appears.
- b. Type the user name and password obtained in [MAP 0000: Start MAP](#) and click *OK*. If the EFCM Basic Edition interface does not open, wait five minutes and perform this step again.

Is the EFCM Basic Edition interface operational?

**NO      YES**

↓      The Internet connection is restored. **Exit MAP.**

Failure of the Ethernet port is indicated. Replace the switch.  
**Exit MAP.**

## MAP 0400: FRU Failure Analysis

This MAP describes fault isolation for product FRUs. The failure indicator is:

- Illumination of the associated amber LED.
- Event code **300, 301, 302, 370, 426, 433, 440, 810, 811, 812, or 850** observed at the *Event Log*.

## 1

[Table 3-6](#) lists event codes, explanations, and MAP steps.

Table 3-6 MAP 400 Event Codes

Event Code	Explanation	Action
300	Cooling fan propeller failed.	Go to <a href="#">step 2</a> .
301	Cooling fan propeller failed.	Go to <a href="#">step 2</a> .
302	Cooling fan propeller failed.	Go to <a href="#">step 2</a> .
370	Cooling fan status polling temporarily disabled.	Go to <a href="#">step 3</a> .
426	Multiple ECC single-bit errors occurred.	Go to <a href="#">step 4</a> .
433	Non-recoverable Ethernet fault.	Go to <a href="#">step 5</a> .
440	Embedded port hardware failed.	Go to <a href="#">step 5</a> .
810	High temperature warning (CTP thermal sensor).	Go to <a href="#">step 6</a> .
811	Critically hot temperature warning (CTP thermal sensor).	Go to <a href="#">step 6</a> .
812	CTP card shutdown due to thermal violations.	Go to <a href="#">step 6</a> .
850	Switch shutdown due to CTP thermal violations.	Go to <a href="#">step 6</a> .

## 2

Visual inspection or event code **300**, **301**, or **302** indicates one or more cooling fans failed. Replace the switch. **Exit MAP.**

## 3

As indicated by event code **370**, cooling fan status polling is temporarily disabled and status values for one or more fans exceed a set threshold. This indicates possible fan degradation or failure.

Is this event code a recurring problem?

**NO**      **YES**



A fan failure is indicated. **Go to [step 2](#).**

Monitor fan operation or recording of additional failure event codes. **Exit MAP.**

**4**

As indicated by event code **426**, an intermittent synchronous dynamic random access memory (SDRAM) problem may result in switch failure.

Is this event code a recurring problem?

**NO**    **YES**

↓    A CTP card failure is indicated. Replace the switch.  
**Exit MAP.**

Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

**5**

As indicated by event code **433** or **440**, the CTP card failed. Replace the switch. **Exit MAP.**

**6**

As indicated by event code **810**, **811**, **812**, or **850**, an intermittent thermal problem may result in switch failure. Reset the product. Refer to [IML or Reset Switch](#) for instructions.

Was the maintenance action successful?

**NO**    **YES**

↓    The product is operational. **Exit MAP.**

A CTP card failure is indicated. Replace the switch. **Exit MAP.**

---

## MAP 0500: Port Failure or Link Incident Analysis

This MAP describes fault isolation for small form factor pluggable (SFP) optical transceivers and Fibre Channel link incidents. The failure indicator is:

- Event code **080**, **081**, **083**, **506**, **507**, **512**, **514**, **515**, or **516** observed at the *Event Log*.
- Event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI server attached to the product reporting the problem.
- An error message observed at the *Link Incident Log*.



## 1

Table 3-7 lists event codes, explanations, and MAP steps.

Table 3-7 MAP 500 Event Codes

Event Code	Explanation	Action
080	Unauthorized worldwide name.	Go to <a href="#">step 2</a> .
081	Invalid attachment.	Go to <a href="#">step 3</a> .
083	Port set to inactive state.	Go to <a href="#">step 13</a> .
506	Fibre Channel port failure.	Go to <a href="#">step 16</a> .
507	Loopback diagnostics port failure.	Go to <a href="#">step 17</a> .
512	Optical transceiver nonfatal error.	Go to <a href="#">step 16</a> .
514	Optical transceiver failure.	Go to <a href="#">step 16</a> .
515	Optical digital diagnostics warning threshold exceeded.	Go to <a href="#">step 16</a> .
516	Optical digital diagnostics alarm threshold exceeded.	Go to <a href="#">step 16</a> .
581	Implicit incident.	Go to <a href="#">step 18</a> .
582	Bit error threshold exceeded.	Go to <a href="#">step 18</a> .
583	Loss of signal or loss of synchronization.	Go to <a href="#">step 18</a> .
584	Not operational primitive sequence received.	Go to <a href="#">step 18</a> .
585	Primitive sequence timeout.	Go to <a href="#">step 18</a> .
586	Invalid primitive sequence received for current link state.	Go to <a href="#">step 18</a> .

Table 3-8 lists link incident messages and MAP steps.

Table 3-8 Link Incident Messages

Explanation	Action
Link interface incident - implicit incident.	Go to <a href="#">step 18</a> .
Link interface incident - bit-error threshold exceeded.	Go to <a href="#">step 18</a> .
Link failure - loss of signal or loss of synchronization.	Go to <a href="#">step 18</a> .

Table 3-8 Link Incident Messages (Continued)

Explanation	Action
Link failure - not-operational primitive sequence (NOS) received.	Go to <a href="#">step 18</a> .
Link failure - primitive sequence timeout.	Go to <a href="#">step 18</a> .
Link failure - invalid primitive sequence received for current link state.	Go to <a href="#">step 18</a> .

## 2

As indicated by event code **080**, the eight-byte (16-digit) worldwide name (WWN) is not valid or an unconfigured nickname was used.

- Select *Node List* from the *Product* menu at any view. The *Node List View* displays.
- At the *Port WWN* column, inspect the WWN assigned to the port or attached device.
- The WWN must be entered in (**XX:XX:XX:XX:XX:XX:XX:XX**) format or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Was the maintenance action successful?

**NO**    **YES**

↓    The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 3

As indicated by event code **081**, a port has an invalid attachment.

- At the *Event Log*, examine the first five bytes of event data.
- Byte **0** specifies the port reporting the problem. Byte **4** specifies the invalid attachment reason as listed in [Table 3-9](#).

Table 3-9 Invalid Attachment Reasons and Actions

Byte 4	Invalid Attachment Reason	Action
<b>01</b>	Unknown	Contact the next level of support.
<b>02</b>	ISL connection not allowed.	Go to <a href="#">step 4</a> .
<b>03, 04</b>	Incompatible switch.	Go to <a href="#">step 5</a> .

Table 3-9 Invalid Attachment Reasons and Actions (Continued)

Byte 4	Invalid Attachment Reason	Action
05	Loopback plug connected.	Go to <a href="#">step 6</a> .
06	N-Port connection not allowed.	Go to <a href="#">step 4</a> .
07	Non-McDATA switch at other end.	Go to <a href="#">step 5</a> .
08	E_Port capability disabled.	Go to <a href="#">step 7</a> .
0A	Unauthorized port binding WWN.	Go to <a href="#">step 2</a> .
0B	Unresponsive node.	Go to <a href="#">step 8</a> .
0C	ESA security mismatch.	Go to <a href="#">step 10</a> .
0D	Fabric binding mismatch.	Go to <a href="#">step 11</a> .
0E	Authorization failure reject.	Go to <a href="#">step 8</a> .
0F	Unauthorized switch binding WWN.	Go to <a href="#">step 10</a> .
10	Authentication failure	Go to <a href="#">step 12</a> .
11	Fabric mode mismatch.	Go to <a href="#">step 5</a> .

## 4

A connection is not allowed because of a conflict with the configured port type. An expansion port (E\_Port) is cabled to a Fibre Channel device or a fabric port (F\_Port) is cabled to a director or fabric switch.

- a. Select *Ports* and *Basic Info* from the *Configure* menu at any view. The *Basic Information View* displays.
- b. If necessary, use the vertical scroll bar to display the information row for the port indicating an invalid attachment.
- c. Select (click) the *Type* field and configure the port as follows:
  - Select fabric port (**F\_Port**) if the port is cabled to a device.
  - Select expansion port (**E\_Port**) if the port is cabled to a director or switch (ISL).
- d. Click *OK* or *Activate*.

Was the maintenance action successful?

**NO**    **YES**

↓    The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 5

An ISL connection is not allowed because one of the following mode-mismatch conditions was detected:

- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a legacy McDATA switch at the incorrect exchange link parameter (ELP) revision level.
- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a non-McDATA switch at the incorrect ELP revision level.
- The product is configured to operate in **McDATA Fabric 1.0** mode and is connected to a non-McDATA switch.

Reconfigure the operating mode:

- a. Set the product offline. Refer to [Set Online State](#).
- b. Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.
- c. Select **McDATA Fabric 1.0** or **Open Fabric 1.0** from the *Interop Mode* drop-down list.
  - Select **McDATA Fabric 1.0** if the product is attached *only* to other McDATA directors or switches operating in **McDATA Fabric 1.0** mode.
  - Select **Open Fabric 1.0** if the product is attached to directors or switches produced by open-fabric compliant original equipment manufacturers (OEMs).
- d. Click *OK* or *Activate*.

Was the maintenance action successful?

**NO**    **YES**

↓    The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 6

A loopback (wrap) plug is connected to the port with no diagnostic running. Remove the plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the product.

- If the port is operational with no device attached, both LEDs adjacent to the port extinguish and the port state is *No Light*.
- If the port is operational with a device attached, the blue/green LED illuminates, the amber LED extinguishes, and the port state is *Online*.

Was the maintenance action successful?

**NO      YES**

↓      The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 7

An ISL connection is not allowed because E\_Port capability is disabled. Install the full-fabric PFE key to enable E\_port capability. Refer to [Install PFE Keys \(Optional\)](#). **Exit MAP.**

## 8

The connection timed out because of an unresponsive device or an ISL security violation (authorization failure reject). Check port status and clean fiber-optic components.

- a. Inform the customer the port will be blocked. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.
- b. Block the port. Refer to [Block or Unblock a Port](#).
- c. Clean fiber-optic connectors. Refer to [Clean Fiber-Optic Components](#).
- d. Unblock the port. Refer to [Block or Unblock a Port](#).
- e. Monitor port operation for approximately five minutes.

Was the maintenance action successful?

**NO      YES**

↓      The product port is operational. **Exit MAP.**

## 9

Inspect and service host bus adapters (HBAs).

Was the maintenance action successful?

**NO**    **YES**

↓    The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 10

A connection is not allowed because of a switch binding or exchange security attribute (ESA) feature mismatch. Switch binding parameters must be compatible for both fabric elements. At the EFCM Basic Edition interface, ensure switch binding is enabled, the connection policy is compatible, and switch membership lists are compatible for both elements. Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

Was the maintenance action successful?

**NO**    **YES**

↓    The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 11

A connection is not allowed because of a fabric binding mismatch. Fabric membership lists must be compatible for both elements. At the EFCM Basic Edition interface, ensure fabric binding is enabled and fabric membership lists are compatible for both elements. Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

Was the maintenance action successful?

**NO**    **YES**

↓    The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 12

A connection is not allowed because of a SANtegrity authentication failure. At the EFCM Basic Edition interface, modify the IP address access control list, product-level authentication settings, port-level authentication settings, and challenge handshake authentication protocol (CHAP) sequence to ensure device access to the product. Refer to the *McDATA EFCM Basic Edition User Manual (620-000240)* for instructions.

Was the maintenance action successful?

**NO**    **YES**

↓    The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 13

As indicated by event code **083**, a port is set to an inactive state.

- a. At the *Event Log*, examine the first two bytes of event data.
- b. Byte **0** specifies the port reporting the problem. Byte **1** specifies the inactive reason as listed in [Table 3-10](#).

Table 3-10 Inactive Port Reasons and Actions

Byte 1	Inactive Port Reason	Action
02	Feature key not enabled.	Go to <a href="#">step 14</a> .
03	Switch speed conflict.	Go to <a href="#">step 15</a> .
04	Optics speed conflict.	Go to <a href="#">step 15</a> .

## 14

A port is inactive because Flexport Technology is disabled. Install the Flexport Technology PFE key to enable N\_Port capability. Refer to [Install PFE Keys \(Optional\)](#). **Exit MAP.**

## 15

A port is inactive because the:

- Port cannot operate at the product (backplane) speed.
- Optical transceiver does not support the configured port speed.

Change the port speed to be compatible with the backplane or optical transceiver speed.

- a. Select *Ports* and *Basic Info* from the *Configure* menu at any view. The *Basic Information View* displays.
- b. If necessary, use the vertical scroll bar to display the information row for the inactive port.
- c. Select (click) the *Speed* field and configure the port.
- d. Click *OK* or *Activate*.

Was the maintenance action successful?

**NO**      **YES**

↓      The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 16

As indicated by event codes **506**, **512**, **514**, **515**, or **516**, a port failed and the optical transceiver must be removed and replaced. Refer to [RRP 1: SFP Optical Transceiver](#).

- The procedure is concurrent and performed while the product is operational.
- Replace the transceiver with a transceiver of the same type (shortwave or longwave) and speed.
- Perform an external loopback test. Refer to [External Loopback Test](#).

---

**NOTE:** Event code **514** may generate a call-home event that incorrectly indicates a CTP card failure. Although the optical socket on the CTP card may have failed, replace the transceiver and verify operation. If a failure is still indicated, replace the switch. When event code **514** is indicated, ensure a replacement transceiver and switch are available.

---

Was the maintenance action successful?

**NO**      **YES**

↓      The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**



## 17

As indicated by event code **507**, a port failed a loopback test. Reset the failed port.

- a. At the EFCM Basic Edition interface:
  1. Select *Ports* and *Reset* from the *Maintenance* menu at any view. The *Reset View* displays.
  2. If necessary, use the vertical scroll bar to display the information row for the port.
  3. Select (click) the check box in the *Reset* column.
  4. Click *OK*. The port resets.
- b. Perform an external loopback test for the reset port. Refer to [External Loopback Test](#).

Was the maintenance action successful?

**NO YES**

↓ The product port is operational. **Exit MAP.**

Go to [step 16](#).

## 18

A message appeared in the *Link Incident Log* or an event code **581**, **582**, **583**, **584**, **585**, or **586** was observed at the console of an OSI server attached to the product reporting the problem. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES NO**

↓ The problem is transient and the product port is operational. **Exit MAP.**

## 19

Clean fiber-optic components.

- a. Inform the customer the port will be blocked. Ensure the system administrator quiets Fibre Channel frame traffic and sets attached devices offline.
- b. Block the port. Refer to [Block or Unblock a Port](#).
- c. Clean fiber-optic connectors. Refer to [Clean Fiber-Optic Components](#).

- d. Unblock the port. Refer to [Block or Unblock a Port](#).
- e. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES NO**

↓ The product port is operational. **Exit MAP.**

## 20

Disconnect the fiber-optic jumper cable from the port and connect the cable to a spare port.

Is a link incident reported at the new port?

**YES NO**

↓ The port reporting the problem is causing the link incident. This indicates port degradation and a possible pending failure. **Go to step 16.**

## 21

Ensure the attached fiber-optic jumper cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

- a. Inform the customer the port will be blocked. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.
- b. Block the port. Refer to [Block or Unblock a Port](#).
- c. Remove and replace the fiber-optic jumper cable.
- d. Unblock the port. Refer to [Block or Unblock a Port](#).

Was the maintenance action successful?

**NO YES**

↓ The product port is operational. **Exit MAP.**

## 22

The attached device is causing the recurrent link incident. Inform the customer of the problem and have the system administrator:

- a. Inspect and verify operation of the attached device.
- b. Repair the attached device if a failure is indicated.
- c. Monitor port operation for approximately five minutes.

Was the maintenance action successful?

**NO**    **YES**

↓    The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## MAP 0600: Fabric or ISL Problem Analysis

This MAP describes fault isolation for fabric, interswitch link (ISL), fenced E\_Port, and segmented E\_Port problems. The failure indicator is an event code **011, 021, 051, 061, 062, 063, 070, 071, 072, 082, 140, 142, or 150** observed at the *Event Log*.

### 1

[Table 3-11](#) lists event codes, explanations, and MAP steps.

Table 3-11    MAP 600 Event Codes

Event Code	Explanation	Action
011	Login Server database invalid.	Go to <a href="#">step 2</a> .
021	Name Server database invalid.	Go to <a href="#">step 2</a> .
051	Management Server database invalid.	Go to <a href="#">step 3</a> .
061	Fabric Controller database invalid.	Go to <a href="#">step 4</a> .
062	Maximum interswitch hop count exceeded.	Go to <a href="#">step 5</a> .
063	Remote switch has too many ISLs.	Go to <a href="#">step 6</a> .
070	E_Port is segmented.	Go to <a href="#">step 7</a> .
071	Switch is isolated.	Go to <a href="#">step 7</a> .
072	E_Port connected to unsupported switch.	Go to <a href="#">step 15</a> .
082	Port fenced.	Go to <a href="#">step 16</a> .
140	Congestion detected on an ISL.	Go to <a href="#">step 21</a> .
142	Low BB_Credit detected on an ISL.	Go to <a href="#">step 21</a> .
150	Fabric merge failure.	Go to <a href="#">step 22</a> .

## 2

A minor error occurred that caused the Fabric Services database to be re-initialized to an empty state, and a disruptive fabric logout and login occurred for all attached devices. Indications are:

- **Event code 011** - The Login Server database failed cyclic redundancy check (CRC) validation.
- **Event code 021** - The Name Server database failed CRC validation.

Devices resume operation after fabric login. Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

## 3

As indicated by event code **051**, a minor error occurred that caused the Management Server database to be re-initialized to an empty state and fail CRC validation. A disruptive server logout and login occurred for all attached devices.

Devices resume operation after Management Server login. Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

## 4

As indicated by event code **061**, a minor error occurred that caused the Fabric Controller database to be re-initialized to an empty state and fail CRC validation. The product briefly lost interswitch link capability.

Interswitch links resume operation after CTP reset. Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

## 5

As indicated by event code **062**, Fabric Controller software detected a path to another fabric element (director or switch) that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Was the maintenance action successful?

**NO**    **YES**

↓      The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 6

As indicated by event code **063**, Fabric Controller software detected a fabric element with more than the allowed number of ISLs. Fibre Channel frames may be lost or directed in loops because of potential fabric routing problems.

Advise the customer of the problem and reconfigure the fabric so that no directors or switches have more than the proscribed number of ISLs.

Was the maintenance action successful?

**NO**    **YES**

↓      The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 7

Event code **070** indicates an E\_Port detected an incompatibility with an attached fabric element, segmented the port, and prevented fabric participation. A segmented E\_port cannot transmit Class 2 or Class 3 Fibre Channel traffic. Event code **071** indicates the product is isolated from all fabric elements, and is accompanied by an event code **070** for each segmented E\_Port. Event code **071** is resolved when all **070** events are corrected. Obtain supplementary event data as follows:

- a. At the *Event Log*, examine the first five bytes of event data.
- b. Byte **0** specifies the segmented E\_port. Byte **4** specifies the segmentation reason as listed in [Table 3-12](#). The reason also displays at the *Port List View*.

Table 3-12 E\_Port Segmentation Reasons and Actions

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to <a href="#">step 8</a> .
02	Duplicate domain ID.	Go to <a href="#">step 9</a> .
03	Incompatible zoning configurations.	Go to <a href="#">step 10</a> .
04	Build fabric protocol error.	Go to <a href="#">step 11</a> .
05	No principal switch.	Go to <a href="#">step 13</a> .
06	No response from attached switch (hello timeout).	Go to <a href="#">step 14</a> .

## 8

An E\_Port segmented because the error detect time out value (E\_D\_TOV) or resource allocation time out value (R\_A\_TOV) is incompatible with the attached fabric element.

- a. Contact customer support or engineering personnel to determine the recommended E\_D\_TOV and R\_A\_TOV values for both fabric elements.
- b. Inform the customer both products will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.
- c. Set both products offline. Refer to [Set Online State](#).
- d. Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.
- e. Type the recommended E\_D\_TOV and R\_A\_TOV values, then click *OK* or *Activate*.
- f. Repeat steps **d** and **e** at the second product (attached to the segmented E\_Port). Use the same E\_D\_TOV and R\_A\_TOV values.
- g. Set both products online. Refer to [Set Online State](#).

Was the maintenance action successful?

**NO**    **YES**

↓    The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 9

An E\_Port segmented because two fabric elements had duplicate domain IDs.

- a. Determine the desired domain ID (**1** through **31** inclusive) for each product.
- b. Inform the customer both products will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.
- c. Set both products offline. Refer to [Set Online State](#).
- d. Select *Switch* and *Parameters* from the *Configure* menu at any view. The *Parameters View* displays.
- e. Type the customer-determined preferred domain ID value, then click *OK* or *Activate*.
- f. Repeat steps **d** and **e** at the second product (attached to the segmented E\_Port). Use a different preferred domain ID value.
- g. Set both products online. Refer to [Set Online State](#).

Was the maintenance action successful?

**NO**    **YES**

↓    The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 10

An E\_Port segmented because two products had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both products, but the zones contain different members.

- a. Determine the desired zone name change for one of the affected products. Zone names must conform to the following rules:
  - The name must be 64 characters or fewer in length.
  - The first character must be a letter (**a** through **z**), upper or lower case.
  - Other characters must be alphanumeric (**a** through **z** or **0** through **9**), dollar sign (**\$**), hyphen (**-**), caret (**^**), or underscore (**\_**).

- b. At the EFCM Basic Edition interface, inspect names in the active zone set to determine the incompatible zone name, then modify the name as directed by the customer. Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

Was the maintenance action successful?

**NO YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 11

An E\_Port segmented because a build fabric protocol error was detected.

- a. Disconnect the fiber-optic jumper cable from the segmented E\_Port.
- b. Reconnect the cable to the same port.

Was the maintenance action successful?

**NO YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

## 12

Reset the product. Refer to *IML or Reset Switch* for instructions.

Was the maintenance action successful?

**NO YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collect Maintenance Data*. **Exit MAP.**

## 13

An E\_Port segmented because no product in the fabric is capable of becoming the principal switch.

- a. Inform the customer the product will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.
- b. Set the product offline. Refer to *Set Online State*.
- c. Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.



- d. At the *Switch Priority* field, select *Principal*, *Never Principal*, or *Default*, then click *OK* or *Activate*. The switch priority value designates the fabric's principal switch, which is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

*Principal* is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means the fabric element is incapable of becoming a principal switch. If all elements are set to *Principal* or *Default*, the element with the highest priority and the lowest WWN becomes the principal switch. At least one element in a multiswitch fabric must be set as *Principal* or *Default*. If all elements are set to *Never Principal*, all ISLs segment.

- e. Set the product online. Refer to [Set Online State](#).

Was the maintenance action successful?

**NO**      **YES**

↓      The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 14

An E\_Port segmented (operational product) because a response (hello timeout) to a verification check indicates an attached switch is not operational.

- a. Perform a data collection at the operational product and contact the next level of support. Refer to [Collect Maintenance Data](#).
- b. Go to [MAP 0000: Start MAP](#) and perform fault isolation for the failed switch. **Exit MAP.**

## 15

Event code **072** indicates a product E\_Port is connected to an unsupported fabric element. Advise the customer of the problem and disconnect the ISL to the unsupported fabric element. **Exit MAP.**

## 16

Event code **082** is informational only and indicates a product E\_Port is fenced (blocked). An application or hardware malfunction occurred (as indicated by failure symptoms or primary event codes) or the port fencing policy is too restrictive. Obtain supplementary event data as follows:

- a. At the *Event Log*, examine the first five bytes (**0** through **4**) of event data.
- b. Byte **0** specifies the E\_Port reporting the problem. Byte **4** specifies the port fence code as listed in [Table 3-13](#).

Table 3-13 Port Fence Codes and Actions

Byte 4	Port Fence Code	Action
01	Protocol error.	Go to <a href="#">step 17</a> .
02	Link-level hot I/O.	Go to <a href="#">step 18</a> .
03	Security violation.	Go to <a href="#">step 19</a> .

## 17

An E\_Port is fenced because of a protocol error. Depending on failure cause, additional information and event codes are available at the product or attached switch. Perform one of the following:

- The E\_Port is segmented and accompanied by primary event code **070**. **Go to [step 7](#)**.
- The fiber-optic cable is disconnected, the cable failed or is degraded, or the port optical transceiver failed. The failure is accompanied by a primary event code indicating the failure type. Go to [MAP 0000: Start MAP](#) and perform fault isolation for the primary event code. **Exit MAP.**
- The E\_Port is fenced because of persistent incomplete operations (ISL bouncing). Go to [MAP 0000: Start MAP](#) and perform fault isolation at the attached switch. **Exit MAP.**
- The E\_Port is fenced because of application-layer protocol errors. Go to [MAP 0000: Start MAP](#) and perform fault isolation at the attached switch. **Exit MAP.**

## 18

An E\_Port is fenced because devices connected to the attached fabric element are flooding the ISL with frames (hot I/O). These link-level problems are typically associated with legacy devices, arbitrated loop devices, or magnetic tape drives. Perform one of the following:

- Disconnect the ISL. **Exit MAP.**
- Refer to the manufacturer's documentation and perform fault isolation at the attached device or fabric element. **Exit MAP.**
- Change port fencing threshold settings to more lenient values. **Go to step 20.**

## 19

An E\_Port is fenced because of persistent firmware-related security violations (SANtegrity binding or SANtegrity authentication failures).

- At the EFCM Basic Edition interface change binding membership lists or authentication parameters as directed by the customer. Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.
- Unblock the port. Refer to [Block or Unblock a Port](#).

Was the maintenance action successful?

**NO**    **YES**

↓    The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 20

Port fencing threshold settings are too restrictive.

- At the EFCM Basic Edition interface, change port fencing threshold settings to more lenient values as directed by the customer. Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.
- Unblock the port. Refer to [Block or Unblock a Port](#).

Was the maintenance action successful?

**NO**    **YES**

↓    The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 21

Event codes **140** and **142** occur only if the optional OpenTrunking feature is enabled.

- **Event code 140** - OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.

- **Event code 142** - OpenTrunking firmware detected an ISL with no transmission BB\_Credit for a period of time that exceeded the configured low BB\_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If the event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the fabric elements reporting the problem.
- Increase the ISL link speed between the fabric elements reporting the problem (from 1 Gbps to 2 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Was the maintenance action successful?

**NO**      **YES**

↓      The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 22

Event code **150** indicates a fabric merge process failed during ISL initialization. An incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes event code **070**, and represents the reply of an adjacent fabric element in response to a zone merge frame. Obtain supplementary event data as follows:

- At the *Event Log*, examine the first 12 bytes (**0** through **11**) of event data.
- Bytes **0** specifies the E\_Port reporting the problem. Bytes **8** through **11** specify the failure reason as listed in [Table 3-14](#).

Table 3-14 Fabric Merge Failure Reasons and Actions

Bytes 8 - 11	Merge Failure Reason	Action
01	Invalid data length.	Go to <a href="#">step 23</a> .
08	Invalid zone set format.	Go to <a href="#">step 23</a> .
09	Invalid data.	Go to <a href="#">step 24</a> .
0A	Cannot merge.	Go to <a href="#">step 24</a> .

Table 3-14 Fabric Merge Failure Reasons and Actions (Continued)

Bytes 8 - 11	Merge Failure Reason	Action
F0	Retry limit reached.	Go to <a href="#">step 23</a> .
F1	Invalid response length.	Go to <a href="#">step 23</a> .
F2	Invalid response code.	Go to <a href="#">step 23</a> .

## 23

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Reason 01** - An invalid data length condition caused an error in a zone merge frame.
- **Reason 08** - An invalid zone set format caused an error in a zone merge frame.
- **Reason F0** - A retry limit reached condition caused an error in a zone merge frame.
- **Reason F1** - An invalid response length condition caused an error in a zone merge frame.
- **Reason F2** - An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E\_Port reporting the problem, then reconnect the cable to the same port.

Was the maintenance action successful?

**NO**      **YES**

↓      The fabric, ISL, and product are operational. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to [Collect Maintenance Data](#). **Exit MAP.**

## 24

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Reason 09** - Invalid data caused a zone merge failure.
- **Reason 0A** - A *Cannot Merge* condition caused a zone merge failure.

Obtain supplementary error code data for event code **150**. At the *Event Log*, examine bytes **12** through **15** of event data that specify the error code. Record the error code.

Perform a data collection and contact the next level of support. Refer to *Collect Maintenance Data*. Report the event code, associated failure reason, and supplementary error code. **Exit MAP.**

This chapter describes repair-related procedures for the Sphereon 4300 Fabric Switch. The procedures are performed at the switch or a browser-capable PC communicating with the product-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface. The chapter describes:

- Procedural notes.
- Powering the switch on or off.
- Cleaning fiber-optic components.
- Downloading firmware from the Filecenter.
- Port light-emitting diode (LED) diagnostics.
- Repair procedures - EFCM Basic Edition.

---

## Procedural Notes

Observe the following procedural notes:

1. Follow all electrostatic discharge (ESD) precautions and **DANGER**, **CAUTION**, and **ATTENTION** statements.
2. Before performing a procedure, read the procedure carefully and thoroughly to familiarize yourself with the information.

## Power On Switch

To power on the switch:

1. An alternating current (AC) power cord is required for the power supply. Ensure the correct power cord is available.



### **DANGER**

***Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.***

2. Plug the power cord into a facility power source and the AC connector at the rear of the switch. When the power cord is connected, the switch powers on and performs power-on self-tests (POSTs).
3. During POSTs:
  - The green **PWR** LED on the switch front panel illuminates.
  - The amber **ERR** LED on the switch front panel blinks momentarily while the switch is tested.
  - The green LED associated with the Ethernet port blinks momentarily while the port is tested.
  - The blue/green and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
4. After successful POST completion, the **PWR** LED remains illuminated and all amber LEDs extinguish.
5. If a POST error occurs, go to [MAP 0000: Start MAP](#) to isolate the problem.



---

## Power Off Switch

To power off the switch:

1. Inform the customer the switch is to be powered off. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline. For instructions, refer to [Set Online State](#).
3. Disconnect the power cord from the AC connector at the rear of the switch.

---

## IML or Reset Switch

An initial machine load (IML) or reset is performed at the switch front panel using the **IML/RESET** button. An IML does not cause power-on diagnostics to execute and is not disruptive to Fibre Channel traffic. An IML:

- Reloads switch firmware from FLASH memory.
- Resets the Ethernet LAN interface, causing the connection to the browser PC or management server to drop momentarily until the connection automatically recovers.

A reset is disruptive to Fibre Channel traffic and resets the:

- Microprocessor and functional logic for the control processor (CTP) card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the browser PC or management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

---

**ATTENTION !** A reset should only be performed if a CTP card failure is indicated. Do not reset a switch unless directed to do so by a procedural step or the next level of support.

---

---

**IML**

To IML the switch:

1. Press and hold the **IML/RESET** button (about three seconds) until the amber **ERR** LED blinks at twice the unit beaconing rate.
2. Release the button. During the IML, the switch-to-browser PC (or management server) Ethernet link drops momentarily.

---

**Reset**

To reset the switch:

1. Press and hold the **IML/RESET** button for ten seconds.
  - After holding the button for three seconds, the amber **ERR** LED blinks at twice the unit beaconing rate.
  - After holding the button for ten seconds, the **ERR** LED stops blinking, and all front panel LEDs illuminate.
2. Release the button to reset the switch. During the reset:
  - The green **PWR** LED on the switch front panel illuminates.
  - The amber **ERR** LED on the switch front panel blinks momentarily while the switch is tested.
  - The green LED associated with the Ethernet port blinks momentarily while the port is tested.
  - Blue/green and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
  - The switch-to-browser PC (or management server) Ethernet link drops momentarily.

---

## Clean Fiber-Optic Components

Perform this procedure as directed by a service procedural step or when connecting or disconnecting fiber-optic cables from port optical transceivers. The following tools (supplied by service personnel) are required:

- ESD grounding cable and wrist strap.
- Fiber-optic cleaning kit with:
  - Oil-free compressed air or HFC-134a aerosol duster.
  - Alcohol-soaked cleaning pads.



### CAUTION

#### Wear eye protection when using an aerosol duster.

To clean fiber-optic components:

1. Optical transceivers are ESD-sensitive. Ensure an ESD grounding cable is connected to the product chassis and your wrist.
2. Disconnect the fiber-optic cable from the optical transceiver as directed by a customer representative or service procedural step.
3. Use an aerosol duster to blow any contaminants from the component (part 1 of [Figure 4-1](#)).
  - Hold the duster upright and keep the air nozzle approximately 50 millimeters (two inches) from the end of the component.
  - For approximately five seconds, continuously blow compressed air or HFC-134a gas on exposed surfaces and the end-face of the component.

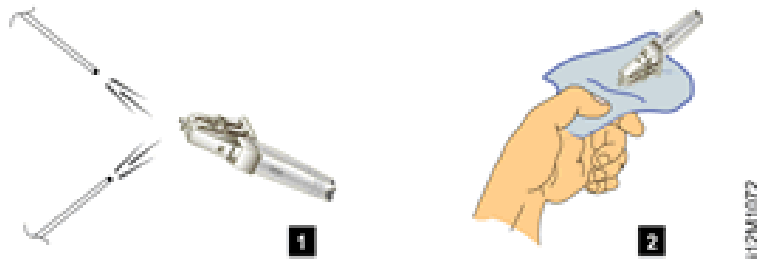


Figure 4-1 Clean Fiber-Optic Components

4. Gently wipe the end-face and other surfaces of the component with an alcohol pad (part 2 of [Figure 4-1](#)). Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for cleaned surfaces to dry.
5. Repeat steps two and three (second cleaning).
6. Repeat steps two and three (third cleaning).
7. Reconnect the fiber-optic cable to the optical transceiver.

## Download Firmware from the Filecenter

The firmware version shipped with the product is provided on the *System Version XX.YY.ZZ* CD-ROM. Subsequent (upgrade) firmware versions are provided to customers through the McDATA Filecenter.

**NOTE:** When upgrading firmware, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the version. Such information supplements information provided in this general procedure.

Download the firmware version to the hard drive of a server with Internet access. This server can be the PC communicating with the EFCM Basic Edition interface. To download a firmware version:



1. At the server with Internet access, open the McDATA home page (<http://mcddata.com>). Select *File Center* from the *Support* menu. The Filecenter home page opens (Figure 4-2).



116M2006

Figure 4-2 McDATA Filecenter Home Page

2. Select (click) *Login* at the top of the page. The *Login* page displays.
3. Type a user name and password (assigned and registered while performing *Task 8: Register with the McDATA File Center*) and click *Login*. The *Welcome, you have been logged in* page displays.

4. Select (click) *Documents* at the top of the page. The *Search / New Documents / By Category* page displays.
5. Select (highlight) the desired option (firmware) from the list box and click *Search*. The *Documents Match* page displays with a list of firmware available for download.
6. As the secure symbol (  ) in the *Status* column indicates, authorization to download a firmware version requires approval. In the *Action* column adjacent to the desired version, click *Add to Request*. The *Current Request: Not Yet Submitted* page displays.
7. At the *Associated Serial Number* field, type the serial number of the product to which the firmware download applies and click *Submit Request*. The *Request Submitted* page displays and the request for approval is e-mailed to support personnel.
8. Wait approximately five minutes for a response, then select (click) *My Requests* at the top of the page. The *Request History* page displays with the approved request (indicated by an approved symbol (  ) in the *Status* column).
9. In the *Action* column adjacent to the approved request for the firmware version, click *Download*. The *File Download* dialog box displays.
10. Click *Save*. The *Save As* dialog box appears.
11. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field, the correct file is specified in the *File name* field, and click *Save*.
12. A *Download* dialog box displays, showing the estimated time remaining to complete the firmware download process. When the process finishes, the dialog box changes to a *Download complete* dialog box.
13. Click *Close* to close the dialog box. The new firmware version is downloaded and saved to the server hard drive.
14. At the server, close the Internet session.
15. If required, transfer the downloaded file from the server to the PC communicating with the EFCM Basic Edition interface. Use a diskette, CD-ROM, or other electronic means.

## Port LED Diagnostics

Fibre Channel port diagnostic information is obtained by inspecting port LEDs at the product front panel or emulated port LEDs at the management interface (EFCM Basic Edition interface). LEDs adjacent to each port and software alert symbols indicate operational status as described in [Table 4-1](#).

Table 4-1 Port Operational States

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Online	On or Blinking	Off	None	An attached device is ready to communicate, or is communicating with other devices.  For online port at 1.0625 Gbps, blue/green LED illuminates green. For online port at 2.125 Gbps, blue/green LED illuminates blue.
Offline	Off	Off	None	Port is blocked and transmitting the offline sequence (OLS) to attached device.
	Off	Off	Yellow Triangle	Port is unblocked and receiving the OLS, indicating attached device is offline.
Beaconing	Off, On, or Blinking	Blinking	Yellow Triangle	Port is beaconing. Amber LED blinks once every two seconds to enable users to locate port.
Invalid Attachment	On	Off	Yellow Triangle	Port has an invalid attachment. Reason appears as supplementary data in the <i>Event Log</i> .
Link Incident	Off	Off	Yellow Triangle	Link incident occurred. Reason appears in the <i>Link Incident Log</i> .
Link Reset	Off	Off	Yellow Triangle	Product and attached device are performing a link reset to recover the connection. Transient state that does not persist.
No Light	Off	Off	None	No signal (light) is received at product port. Normal condition when no cable is attached to port or when attached device is powered off.
Inactive	On	Off	Yellow Triangle	Port is inactive. Reason appears at <i>Port List View</i> or <i>Port Properties</i> dialog box.
Not Installed	Off	Off	None	Optical transceiver not installed in the port.
Not Operational	Off	Off	Yellow Triangle	Port is receiving the not operational sequence (NOS) from attached device.

Table 4-1 Port Operational States (Continued)

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Port Failure	Off	On	Red and Yellow Blinking Diamond	Port failed and requires service.
Segmented E_Port	On	Off	Yellow Triangle	E_Port segmented, preventing connected switches from forming a fabric. Reason appears as supplementary data in the <i>Event Log</i> .
Testing	Off	Blinking	Yellow Triangle	Port is performing an internal loopback test.
	On	Blinking	Yellow Triangle	Port is performing an external loopback test.

## Repair Procedures - EFCM Basic Edition

The following procedures (performed at a PC communicating with the EFCM Basic Edition interface) are described:

- Obtain log information.
- Perform port diagnostics.
- Collect maintenance data.
- Set online state.
- Block or unblock a port.
- Upgrade firmware.
- Manage configuration data.

### Obtain Log Information

The EFCM Basic Edition interface provides access to logs that contain maintenance information. Select the desired log from the *Logs* menu at any view. Logs with maintenance information are:

- Event.
- Link Incident.
- Open Trunking Re-Route.
- Fabric.
- Embedded Port Frame.

**Event Log** The *Event Log* records events or errors. Entries reflect the status of the management interface and managed product. The log describes:

- **Date/Time** - Date and time the event occurred.
- **Error Code** - Three-digit code that describes the event. Event codes are listed and described in [Appendix A, Event Code Tables](#).
- **Severity** - Event severity (*Informational, Minor, Major, or Severe*).
- **Event Data** - Supplementary information (if available) in hexadecimal format. Event data is described in [Appendix A, Event Code Tables](#).

**Link Incident Log** The *Link Incident Log* records Fibre Channel link incident events and causes. The log describes:

- **Date/Time** - Date and time the link incident occurred.
- **Port** - Port number reporting the link incident.
- **Link Incident Event** - Brief description of the link incident and cause, including:
  - Implicit incident.
  - Bit-error threshold exceeded.
  - Loss of signal or loss of synchronization.
  - Not-operational primitive sequence received.
  - Primitive sequence timeout.
  - Invalid primitive sequence received for current link state.

Refer to [MAP 0500: Port Failure or Link Incident Analysis](#) for corrective actions.

**Open Trunking Re-Route Log**

The *Open Trunking Re-Route Log* records interswitch link (ISL) congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed product. The log describes:

- **Date/Time** - Date and time the re-route occurred.
- **Receive Port** - Target port number (decimal) receiving Fibre Channel traffic after the re-route.
- **Target Domain** - Target device domain ID (decimal) receiving Fibre Channel traffic after the re-route.



- **Old Exit Port** - Port number (decimal) transmitting Fibre Channel traffic before the re-route.
- **New Exit Port** - Port number (decimal) transmitting Fibre Channel traffic after the re-route.

#### Fabric Log

The *Fabric Log* records the time and nature of changes made to a multiswitch fabric. The information is useful for isolating zoning or fabric-wide problems. The log describes:

- **Count** - Cumulative count of log entries (wrapping or non-wrapping).
- **Date/Time** - Date and time the change occurred.
- **Description** - Description of the zoning or fabric change.
- **Data** - Supplementary information (if available) in text format.

---

**NOTE:** Identical entries are recorded in the wrapping and non-wrapping logs. When the non-wrapping log fills, old records are overwritten. The wrapping log preserves all records.

---

#### Embedded Port Frame Log

The Embedded Port Frame Log records all Fibre Channel frames transmitted through the product's embedded port, including Class F traffic, fabric logins, state change notifications, and exception frames. The information is useful for Fibre Channel frame debugging (usually performed by second-level support. The log describes:

- **Count** - Cumulative count of log entries (wrapping or non-wrapping).
- **Date/Time** - Date and time frame was transmitted through the embedded port.
- **Port #** - Fibre Channel port number (decimal) transmitting frame through the embedded port.
- **Direction** - Fibre Channel frame direction - incoming (**I**) or outgoing (**O**).
- **SOF** - Start of frame character (hexadecimal).
- **EOF** - End of frame character (hexadecimal).
- **Payload Size** - Size of frame payload in bytes.
- **Header** - 24-byte frame header (hexadecimal).
- **Payload** - First 32 bytes of frame payload (hexadecimal).

## Perform Port Diagnostics

Fibre Channel port diagnostic information is obtained by:

- Inspecting port properties, predictive optics monitoring (POM) data, or port transceiver technology information at the lower panel of the *Port List View*.
- Inspecting port statistics information at the *Performance View*.
- Performing an internal or external loopback test.

### Port List View

The EFCM Basic Edition interface provides access to port diagnostic information through the *Port List View*. To open this view, select *Port List* from the *Product* menu at any view. As an example, the figure shows POM data in the lower panel ([Figure 4-3](#)).

The screenshot shows the 'Product > Port List' interface. At the top, there is a 'Jump to Port:' field with '0' entered and a 'go' button. Below this is a table with columns: Port, Name, Block Configuration, Operational State, Type, Health Status, and Transceiver. The table lists ports 0 through 10. Port 0 is selected, and its details are shown in a panel below. The panel includes 'Port Number: 0', 'Health Status: Normal', and 'Transceiver Type: SFP'. The main data table in the panel has columns: Measured Result, Temperature [C], Supply Voltage [V], Bias Current [mA], TX Power [uW], and RX Power [uW]. Below this are threshold values for Alarm Max, Warning Max, Warning Min, and Alarm Min for each parameter.

Port	Name	Block Configuration	Operational State	Type	Health Status	Transceiver
0	-	Unblocked	Online	E Port	Normal	SFP
1	-	Unblocked	No Light	Gx Port	Normal	SFP
2	-	Unblocked	No Light	Gx Port	Normal	SFP
3	-	Unblocked	No Light	Gx Port	Normal	SFP
4	-	Unblocked	No Light	Gx Port	Normal	SFP
5	-	Unblocked	No Light	Gx Port	Normal	SFP
6	-	Unblocked	No Light	Gx Port	Normal	SFP
7	-	Unblocked	No Light	Gx Port	Normal	SFP
8	-	Unblocked	No Light	Gx Port	Normal	SFP
9	-	Unblocked	No Light	Gx Port	Normal	SFP
10	-	Blocked	Offline	Gx Port	Normal	SFP

Port Number: 0		Health Status: Normal		Transceiver Type: SFP		
Measured Result	Temperature [C]	Supply Voltage [V]	Bias Current [mA]	TX Power [uW]	RX Power [uW]	
	28.203	3.282	6.320	315.000	218.400	
Thresholds						
Alarm Max	95.000	3.830	28.000	794.300	1000.000	
Warning Max	90.000	3.580	14.800	630.900	794.300	
Warning Min	-25.000	3.040	4.600	141.300	31.000	
Alarm Min	-30.000	2.970	3.100	125.900	25.100	

116M2007

Figure 4-3 Port List View

A row of information for each port appears. Each row consists of the following columns:

- **Port** - Product port number.
- **Name** - Port name of 24 alphanumeric characters or less. The name typically characterizes the device or fabric element to which the port is attached.
- **Block Configuration** - Indicates if a port is blocked or unblocked.

- **Operational State** - Port state (*Online, Offline, Not Installed, Inactive, Invalid Attachment, Link Reset, No Light, Not Operational, Port Failure, Segmented E\_Port, or Testing*).
- **Type** - Configured port type. Settings are:
  - Generic mixed port (GX\_Port). This setting also configures a port as a generic loop port (GL\_Port).
  - Fabric mixed port (FX\_Port). This setting also configures a port as a fabric loop port (FL\_Port).
  - Generic port (G\_Port).
  - Fabric port (F\_Port).
  - Expansion port (E\_Port).
- **Health Status** - Condition of the installed optical transceiver (*Normal, Warning, Alarm, or No Info*).
- **Transceiver** - Installed transceiver type (*SFP, XFP, or Unknown*).

### Inspect Port Properties

At the *Port List View*, click a physical port number listed in the *Port* column. Physical properties for the selected port appear in the lower panel of the view:

- **Port Number** - Product port number.
- **Port Name** - User-defined name or description for the port.
- **Port Type** - User-defined port type (*GX\_Port, FX\_Port, G\_Port, F\_Port, or E\_Port*).
- **Operating Speed** - Port operating speed (*Not Established, 1 Gbps, or 2 Gbps*).
- **Fibre Channel Address** - Port FC address identifier. Port FC address if the port was swapped.
- **Port WWN** - Fibre Channel world wide name (WWN) of the port.
- **Attached Port WWN** - Fibre Channel WWN of the device attached to the port.
- **Block Configuration** - User-configured state for the port (*Blocked or Unblocked*).
- **Beaconing** - User-specified for the port (*On or Off*).

- **FAN Configuration** - User-configured state for fabric address notification (FAN) configuration (*Enabled* or *Disabled*).
- **Operational State** - Port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E\_Port*, *Disabled*, or *Testing*).
- **Reason** - A summary appears describing the reason if the port state is *Segmented E\_Port*, *Invalid Attachment*, or *Inactive*. For any other port state, the reason is *N/A*.

### Inspect POM Data

At the *Port List View*, click the entry for a port in the *Health Status* column. POM data for the selected port appears in the lower panel of the view ([Figure 4-3](#)):

- **Port Number** - Product port number.
- **Health Status** - Condition of the installed optical transceiver (*Normal*, *Warning*, *Alarm*, or *No Info*).
- **Transceiver Type** - Installed transceiver type (*SFP*, *XFP*, or *Unknown*).

If the port has a digital diagnostics (DD) enabled optical transceiver installed, product firmware displays a table of reported temperature, voltage, current, transceiver power, and receiver power. Optical transceivers also provide vendor-specific threshold values for these parameters.

### Inspect Port Transceiver Technology

At the *Port List View*, click the entry for a port in the *Transceiver* column. Port transceiver technology information for the selected port appears in the lower panel of the view:

- **Port Number** - Product port number.
- **Identifier** - Installed transceiver type (*SFP*, *XFP*, or *Unknown*).
- **Connector type** - Type of port connector (*LC*, *MT\_RJ*, *MU*, *Unknown*, or *Internal Port*).
- **Transceiver** - Type of port transceiver (*Shortwave Laser*, *Longwave Laser*, *Long Distance Laser*, *Unknown*, or *None*).
- **Distance Capability** - Port transmission distance (*Short*, *Intermediate*, *Long*, *Very Long*, or *Unknown*).

- **Media** - Type of optical cable used (*Singlemode, multimode 50-micron, multimode 62.5-micron, or Unknown*).
- **Speed** - Operating speed (*Unknown, 1 Gbps, or 2 Gbps*).

### Performance View

The EFCM Basic Edition interface provides access to port statistics information through the *Performance View*. To open this view, select *Performance* from the *Product* menu at any other view. The following information appears:

- **Traffic Statistics** - These statistics include port transmit and receive values for frames; four-byte words; offline sequences; link resets; and link utilization percentage. The time spent using no transmission buffer-to-buffer credit (BB\_Credit) is also reported.
- **Error Statistics** - These statistics include the number of link failures; synchronization and signal losses; discarded frames; invalid transmission words; primitive sequence, cyclic redundancy check (CRC), delimiter, and address identification errors; and short frames.
- **Class 2 Statistics** - These statistics include the number of 4-byte words transmitted and received, and the number of Class 2 frames transmitted, received, busied, or rejected.
- **Class 3 Statistics** - These statistics include the number of 4-byte words transmitted and received, and the number of Class 3 frames transmitted, received, or discarded.
- **Open Trunking Statistics** - These statistics include the number of traffic flows rerouted to or from an ISL due to congestion.

### Internal Loopback Test

An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test. To perform the test:

1. Inform the customer a disruptive internal loopback test is to be performed. Ensure the system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.

---

**NOTE:** A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. A device can remain connected during the test.

---

2. At the EFCM Basic Edition interface, select *Ports* and *Diagnostics* from the *Maintenance* menu at any view. The *Diagnostics View* displays (Figure 4-4).

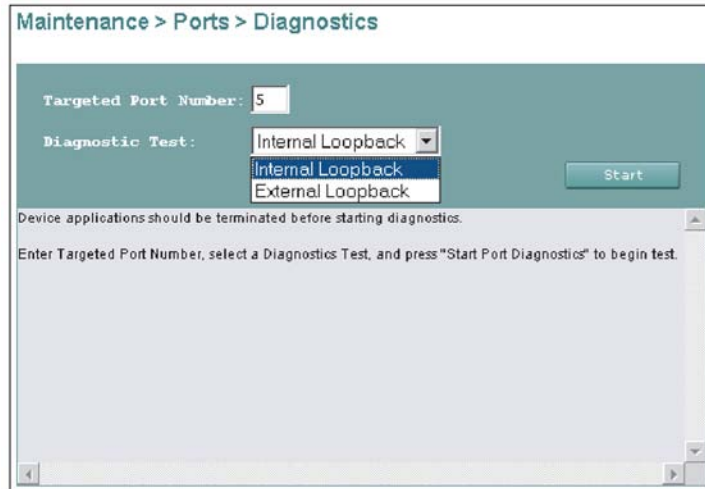


Figure 4-4 Diagnostics View

3. Type the port number to be tested in the *Targeted Port Number* field.
4. At the *Diagnostic Test* list box, select the *Internal Loopback* option.
5. Click *Start*. The test begins and:
  - a. The *Diagnostics View* changes to a *Diagnostics - Executing View*.
  - b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

---

**NOTE:** Click *Stop* at any time to abort the loopback test.

---

6. When the test completes, the *Diagnostics - Executing View* reverts to the *Diagnostics View*. Test results appear as **Passed**, **Failed**, or **Test Incomplete** in the message area of the view.
7. Reset the tested port:
  - a. Select *Ports* and *Reset* from the *Maintenance* menu at any view. The *Reset View* displays.

- b. For the tested port, click (enable) the check box in the *Reset* column. A check mark in the box indicates the port reset option is enabled.
  - c. Click *OK*. The port resets.
8. Inform the customer the test is complete and the attached device can be set online.

### External Loopback Test

An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a singlemode or multimode loopback plug must be inserted in the port. To perform the test:

1. Inform the customer a disruptive external loopback test is to be performed and the attached device must be disconnected.
2. Disconnect the fiber-optic jumper cable from the port to be tested.
3. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
4. At the EFCM Basic Edition interface, select *Ports* and *Diagnostics* from the *Maintenance* menu at any view. The *Diagnostics View* displays (Figure 4-4).
5. Type the port number to be tested in the *Targeted Port Number* field.
6. At the *Diagnostic Test* list box, select the *External Loopback* option.
7. Click *Start*. The test begins and:
  - a. The *Diagnostics View* changes to a *Diagnostics -Executing View*.
  - b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

---

**NOTE:** Click *Stop* at any time to abort the loopback test.

---

8. When the test completes, the *Diagnostics - Executing View* reverts to the *Diagnostics View*. Test results appear as **Passed**, **Failed**, or **Test Incomplete** in the message area of the view.
9. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in [step 2](#)).

10. Reset the tested port:
  - a. Select *Ports* and *Reset* from the *Maintenance* menu at any view. The *Reset View* displays.
  - b. For the tested port, click (enable) the check box in the *Reset* column. A check mark in the box indicates the port reset option is enabled.
  - c. Click *OK*. The port resets.
11. Inform the customer the test is complete and the device can be reconnected and set online.

---

## Collect Maintenance Data

When firmware detects a critical error, the product automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the CTP card. Perform this procedure after a firmware fault or FRU failure to capture data for analysis by support personnel. Maintenance data includes the dump file and engineering logs.

**NOTE:** An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a product feature enablement (PFE) key, a memory dump file (that may include classified Fibre Channel frames) is not included as part of the data collection procedure.

To collect maintenance data:

1. At the EFCM Basic Edition interface, select *System Files* from the *Maintenance* menu at any view. The *System Files View* displays (Figure 4-5).



116M2009

Figure 4-5 System Files View



2. Right-click the *Data Collection* link to open a list of menu options. Select the *Save Target As* menu option. The *Save As* dialog box displays.
3. Insert a blank diskette in the floppy drive of the PC communicating with the EFCM Basic Edition interface.
4. At the *Save As* dialog box, select the floppy drive (A:\) from the *Save in* drop-down menu, type a descriptive name for the zipped (.zip) dump file in the *File name* field, and click *Save*.
5. A *Download* dialog box displays, showing the estimated time remaining to complete the download process. When finished, the dialog box changes to a *Download complete* dialog box.
6. Click *Close* to close the dialog box.
7. Remove the diskette with the newly-collected maintenance data from the PC floppy drive. Return the diskette with the failed FRU to support personnel for failure analysis.

---

## Set Online State

This section describes procedures to set the product online or offline. Operational states are:

- **Online** - When the product is set online, an attached device can log in if the port is not blocked. Attached devices in the same zone can communicate with each other.
- **Offline** - When the product is set offline, all ports are set offline and operation of attached Fibre Channel devices is disrupted. The product transmits the OLS to attached devices, and the devices cannot log in.

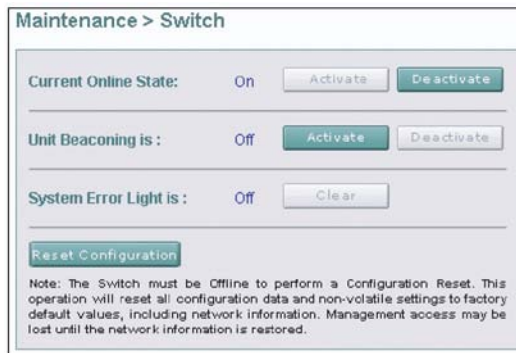
---

**NOTE:** Do not set the product offline unless directed to do so by a procedural step or the next level of support.

---

To set the product online or offline:

1. At the EFCM Basic Edition interface, select *Switch* from the *Maintenance* menu at any view. The *Switch View* displays (Figure 4-6).



i16M2010

Figure 4-6 Switch View

2. Perform one of the following:
  - If the product is offline, click the green *Activate* button adjacent to the *Current Online State*: field. The product comes online.
  - If the product is online, click the green *Deactivate* button adjacent to the *Current Online State*: field. The product goes offline.

---

## Block or Unblock a Port

This section describes procedures to block or unblock a Fibre Channel port. Blocking a port prevents an attached device or fabric element from communicating. A blocked port continuously transmits the OLS. To block or unblock a port:

1. At the EFCM Basic Edition interface, select *Ports* and *Basic Info* from the *Configure* menu at any view. The *Basic Information View* displays (Figure 4-7).

Configure > Ports > Basic Information

Jump to Port:  go

Port	Name	Blocked	FAN	Type	Speed
0	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
1	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
2	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
3	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	F Port	1 G
4	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
5	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	F Port	1 G
6	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
7	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
8	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
9	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate
10	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gx Port	Negotiate

OK Cancel

r16M2011

Figure 4-7 Basic Information View

2. Perform one of the following:
  - Click the check box for the selected port in the *Blocked* column to block the port (default is unblocked). A check mark in the box indicates the port is blocked.
  - Click the check box for the selected port in the *Blocked* column to remove the check mark and unblock the port. A blank box indicates the port is unblocked.
3. Click *OK* to save and activate changes.

## Upgrade Firmware

Firmware is the product operating code stored in FLASH memory on the CTP card. Multiple firmware versions can be stored on a PC hard drive and made available for download through the EFCM Basic Edition interface. Perform the following firmware upgrade tasks at the EFCM Basic Edition interface:

- Determine the active firmware version.
- Download a firmware version.

## Determine Firmware Version

To determine a firmware version, select *Hardware* from the *Product* menu at any view. The *Hardware View* displays. At the bottom of the page, record the firmware version listed in the *Firmware Level* field.

## Download Firmware Version

Ensure the desired firmware version is obtained from the Filecenter and resident on the hard drive of the PC communicating with the EFCM Basic Edition interface. Refer to [Download Firmware from the Filecenter](#) for instructions.

**NOTE:** When upgrading firmware, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the version. Such information supplements information provided in this general procedure.

To download a firmware version:

1. At the EFCM Basic Edition interface, select *Firmware Upgrade* from the *Maintenance* menu at any view. The *Firmware Upgrade View* displays (Figure 4-8).

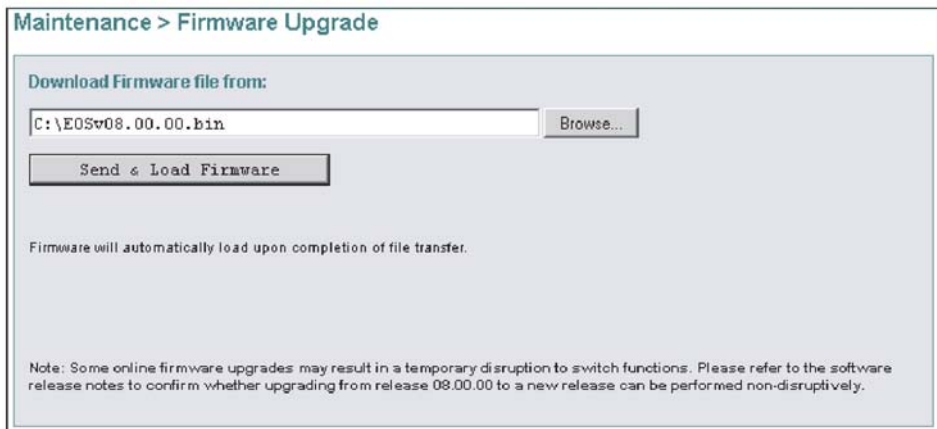


Figure 4-8 Firmware Upgrade View

116M2012

2. At the *Download Firmware file from* field, select the desired file from the PC hard drive using the *Browse* button or type the desired filename.
3. Click *Send and Load Firmware*. A message box displays, indicating any browser operation will terminate the firmware download.
4. Click *OK* to download firmware. The process takes several minutes to complete, during which the browser is unavailable. When the process completes, the message **Firmware successfully received and verified. Your browser connection will be unavailable until unit restart is complete.** displays.
5. After verification, the switch performs an initial program load (IPL) that takes approximately 30 seconds to complete. During the IPL, the browser-to-switch Internet connection drops momentarily and the EFCM Basic Edition session is lost.
6. After the switch IPL and EFCM Basic Edition session logout, the message **Firmware upgrade complete. Click [here](#) to login.** displays.
7. Click [here](#) to login and start a new EFCM Basic Edition session. The *Enter Network Password* dialog box displays.
8. Type the default user name and password.

---

**NOTE:** The default user name is **Administrator** and the default password is **password**. Both are case-sensitive.

---

9. Click *OK*. The EFCM Basic Edition interface opens with the *Hardware View* panel displayed.

---

## Manage Configuration Data

The EFCM Basic Edition interface provides options to:

- Back up and restore the configuration file stored in nonvolatile random-access memory (NV-RAM) on the switch CTP card.
- Reset the configuration file to factory default values.

The switch must be set offline prior to restoring or resetting the configuration file.

## Back Up Configuration

To back up the switch configuration file to the PC communicating with the EFCM Basic Edition interface:

1. Select *Backup Configuration* from the *Maintenance* menu at any view. The *Backup Configuration View* displays (Figure 4-9).

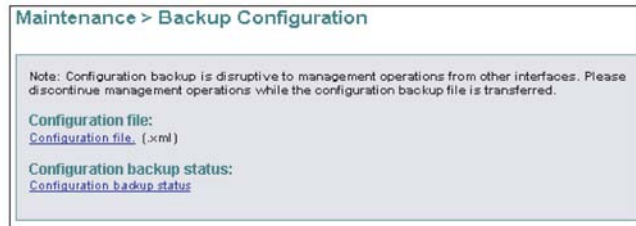


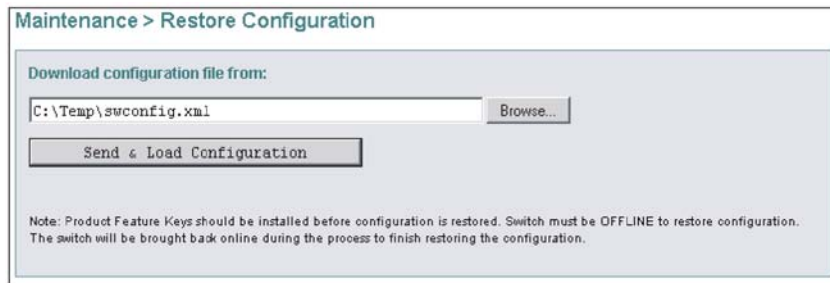
Figure 4-9 Backup Configuration View

2. Right-click the *Configuration file* link to open a list of menu options. Select the *Save Target As* menu option. The *Save As* dialog box displays.
3. At the *Save As* dialog box, select the hard drive (C:\) from the *Save in* drop-down menu, type a descriptive name for the extensible markup language (.xml) configuration file in the *File name* field, and click *Save*.
4. A *Download* dialog box displays, showing the estimated time remaining to complete the backup process. When finished, the dialog box changes to a *Download complete* dialog box.
5. Click *Close* to close the dialog box.

## Restore Configuration

To restore the switch configuration file from the PC communicating with the EFCM Basic Edition interface:

1. Inform the customer the switch is to be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline. For instructions, refer to *Set Online State*.
3. Select *Restore Configuration* from the *Maintenance* menu at any view. The *Restore Configuration View* displays (Figure 4-10).



116M2014

Figure 4-10 Restore Configuration View

4. At the *Download Configuration file from* field, select the desired file from the PC hard drive using the *Browse* button or type the desired filename.
5. Click *Send and Load Configuration*. A message box displays, indicating any browser operation will terminate the configuration download.
6. Click *OK* to download the configuration. The process takes several minutes to complete, during which the browser is unavailable. When the process completes, the message **Configuration restored successfully** displays.

### Reset Configuration Data

When configuration data is reset to factory default values, the switch defaults to the factory-set (Internet Protocol) IP address and all optional features are disabled. To reset configuration data to factory default settings:

1. Inform the customer the switch is to be set offline. Ensure the system administrator quiescs Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. Set the switch offline. For instructions, refer to [Set Online State](#).
3. At the EFCM Basic Edition interface, select *Switch* from the *Maintenance* menu at any view. The *Switch View* displays ([Figure 4-6](#)).
4. Click *Reset Configuration*. A dialog box with the message **Are you sure that you want to reset the configuration?** displays.
5. Click *OK* to reset the configuration.

6. The switch IP address resets to the default address of **10.1.1.10**.
  - If the configured IP address (prior to reset) was the same as the default address, the browser-to-switch Internet connection is not affected and the procedure is complete.
  - If the configured IP address (prior to reset) was not the same as the default address, the browser-to-switch Internet connection drops and the EFCM Basic Edition session is lost. Continue to the next step.
7. To change the switch IP address and restart the EFCM Basic Edition interface, refer to [Configure Network Information](#). To restart the EFCM Basic Edition interface using the default IP address of **10.1.1.10**:
  - a. At the browser, enter the default IP address of **10.1.1.10** as the Internet URL. The *Enter Network Password* dialog box displays.
  - b. Type the default user name and password.

---

**NOTE:** The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---

- c. Click **OK**. The EFCM Basic Edition interface opens and the procedure is complete.



This chapter describes field-replaceable unit (FRU) removal and replacement procedures (RRPs) for the Sphereon 4300 Fabric Switch. The chapter also provides procedural notes, electrostatic discharge (ESD) precautions, and list of FRUs.

## Procedural Notes

Observe the following procedural notes:

1. Follow all ESD precautions and **DANGER**, **CAUTION**, and **ATTENTION** statements.
2. Do not perform an RRP unless a failure is isolated to a FRU. If fault isolation was not performed, refer to [MAP 0000: Start MAP](#).
3. Before removing a FRU, read the associated RRP to familiarize yourself with the procedure.
4. After completing an RRP:
  - Clear the event codes reporting the failure and recovery from the product *Event Log*.
  - Extinguish the amber system error light-emitting diode (LED) at the product front panel.

## ESD Procedures

Follow these ESD procedures:

- If the product is connected to facility power (grounded), wear an ESD wrist strap and grounding cable connected to the product chassis.
- If the product is not connected to facility power (not grounded), wear an ESD wrist strap and grounding cable connected to an approved bench grounding point.
- Touch the product chassis once before performing a procedure, and once each minute during the procedure.
- Store ESD-sensitive FRUs in antistatic packaging.

## Field-Replaceable Units

[Table 5-1](#) lists the concurrent FRU that is removed and replaced while the product is powered on and operational. The table also lists ESD precautions (yes or no) for the FRU, and references the RRP page number. Refer to [Chapter 6, \*Illustrated Parts Breakdown\*](#) for FRU locations and part numbers.

Table 5-1 Concurrent FRU

Concurrent FRU	ESD Requirement	Page
Small form factor pluggable optical transceiver	Yes	5-3

## RRP 1: SFP Optical Transceiver

Use the following procedures to remove or replace a small form factor pluggable (SFP) optical transceiver. A list of required tools is provided.

### Tools Required

The following tools are required:

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Protective cap (provided with the fiber-optic jumper cable).
- Loopback plug (provided with the product).
- Fiber-optic cleaning kit.
- ESD grounding cable and wrist strap.

### Removal

To remove an SFP optical transceiver:

1. Inform the customer the port with the defective transceiver will be blocked. Ensure the system administrator sets any attached device offline.
2. If the product is not rack-mounted, go to [step 3](#). If the product is rack-mounted, perform one of the following:
  - If the product is installed in an FC-512 Fabricenter equipment cabinet, insert the 5/16-inch door tool into the socket hole at the right top of the door (front or rear). Turn the tool counter-clockwise to unlock and open the door.
  - If the product is installed in a customer-supplied equipment cabinet, unlock and open the cabinet door (front or rear) as directed by the customer representative.
3. Identify the defective port transceiver from:
  - An illuminated amber LED adjacent to the port.
  - At a web browser communicating with the EFCM Basic Edition interface, port failure information displayed at the *Hardware View*, *Port List View*, or *Event Log*.
4. Block communication to the port. Refer to [Block or Unblock a Port](#) for instructions.
5. Ensure an ESD grounding cable is connected to the product chassis (or approved bench ground) and your wrist.

6. Disconnect the fiber-optic jumper cable from the port:
  - a. Pull the keyed LC connector free from the port's optical transceiver.
  - b. Place a protective cap over the jumper cable connector.
7. The optical transceiver has a wire locking bale to secure the transceiver in the port receptacle and to assist in removal. The bale rotates up or down, depending on transceiver manufacturer and port location (top or bottom row).
  - a. Disengage the locking mechanism by rotating the wire bale up or down 90 degrees as shown in part (1) of [Figure 5-1](#).
  - b. Grasp the wire bale and pull the transceiver from the port receptacle as shown in part (2) of [Figure 5-1](#).

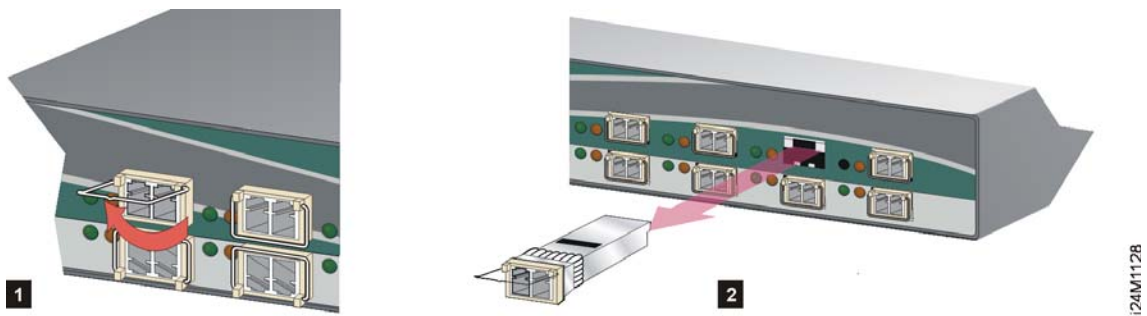


Figure 5-1 SFP Optical Transceiver Removal and Replacement

8. At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu. An event code **513** (SFP optics hot-removal completed) appears in the *Event Log*.

**Replacement** To replace an SFP optical transceiver:

1. Ensure an ESD grounding cable is connected to the product chassis (or approved bench ground) and your wrist.
2. Remove the replacement transceiver from its packaging.
3. Insert the transceiver into the port receptacle, then engage the locking mechanism by rotating the wire bale up or down 90 degrees as shown in [Figure 5-1](#).

4. Perform an external loopback test. Refer to *External Loopback Test* for instructions. If the test fails, go to *MAP 0000: Start MAP* to isolate the problem.
5. Reconnect the fiber-optic jumper cable:
  - a. Remove the protective cap from the cable connector and the protective plug from the port optical transceiver. Store the cap and plug in a suitable location for safekeeping.
  - b. Clean the jumper cable and transceiver connectors. Refer to *Clean Fiber-Optic Components* for instructions.
  - c. Insert the keyed LC cable connector into the port's optical transceiver.
6. Ensure the amber port LED extinguishes. If the LED illuminates, go to *MAP 0000: Start MAP* to isolate the problem.
7. At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu. Ensure an event code **510** (SFP optics hot-insertion initiated) appears. If the event code does not appear, go to *MAP 0000: Start MAP* to isolate the problem.
8. At a web browser communicating with the EFCM Basic Edition interface, open the *Hardware View* and verify port operation:
  - a. Ensure alert symbols do not appear (yellow triangle or red diamond).
  - b. Open the *Port List View*. Verify that port *Operational State*, *Type*, *Health Status*, and *Transceiver* are correct.If a problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem.
9. Restore communication to the port as directed by the customer. Refer to *Block or Unblock a Port* for instructions. Inform the customer the port is available.
10. Clear the system error LED on the product front bezel. At a web browser communicating with the EFCM Basic Edition interface, select *Clear System Error Light* from the *Maintenance* menu.
11. If necessary, close and lock the equipment cabinet door.



This chapter provides an illustrated parts breakdown for Sphereon 4300 Switch field-replaceable units (FRUs). Exploded-view assembly drawings are provided for:

- Front-accessible FRUs.
- Miscellaneous parts.
- Power cords and receptacles.

Exploded-view illustrations portray the switch disassembly sequence for clarity. Illustrated FRUs are numerically keyed to associated tabular parts lists. The parts lists also include McDATA part numbers, descriptions, and quantities.

## Front-Accessible FRUs

Figure 6-1 illustrates front-accessible FRUs. Table 6-1 is the associated FRU parts list. The table includes reference numbers to Figure 6-1, FRU part numbers, descriptions, and quantities.



Figure 6-1 Front-Accessible FRUs

Table 6-1 Front-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
6 - 1	002-002788-002	Switch, Spheron 4300, Version 2, base assembly	Reference
-1	803-000074-386	Transceiver, optical, SFP, 850 nm, 3.3 volt, LC connector, dual-rate (1.0625/2.1250 Gbps), digital diagnostic	0 to 12
-1	803-000075-313	Transceiver, optical, SFP, 1310 nm, 3.3 volt, LC connector, dual-rate (1.0625/2.1250 Gbps), digital diagnostic, 10 km	0 to 12
-1	803-000076-313	Transceiver, optical, SFP, 1310 nm, 3.3 volt, LC connector, dual-rate (1.0625/2.1250 Gbps), digital diagnostic, 20 and 35 km	0 to 12



## Miscellaneous Parts

Figure 6-2 illustrates miscellaneous parts. Table 6-2 is the associated parts list. The table includes reference numbers to Figure 6-2, part numbers, descriptions, and quantities.

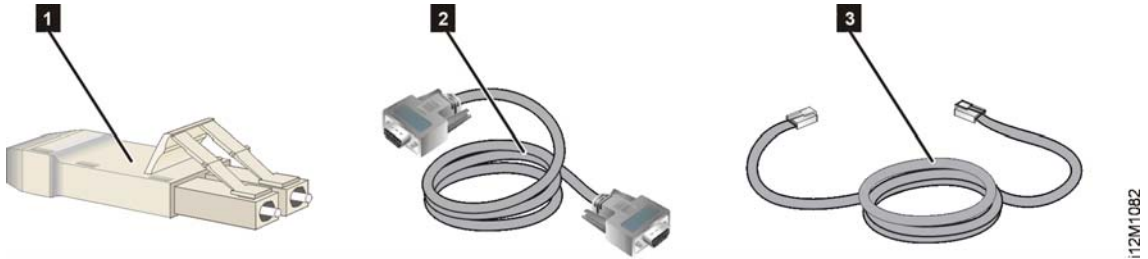


Figure 6-2 Miscellaneous Parts

Table 6-2 Miscellaneous Parts List

Ref.	Part Number	Description	Qty.
-1	803-000057-000	Plug, loopback, LC connector, multimode, 50/125 micron (#1148)	1
-1	803-000057-001	Plug, loopback, LC connector, singlemode, 9/125 micron (#1149)	1
-2	801-000039-000	Cable, communication, null modem, DB9F-DB9F connectors, 10-foot	1
-3	801-000035-010	Cable, Ethernet, RJ-45 connectors, Category 5E, 10-foot	1

## Power Cords and Receptacles

Figure 6-3 illustrates optional power cords and receptacles. Table 6-3 is the associated parts list. The table includes reference numbers to Figure 6-3, feature numbers, and descriptions.













1		7, 11, 14	
2		8	
3		9	
4		10	
5		12, 13	
6		15	

Figure 6-3 Power Cords and Receptacles

i12M1083

Table 6-3 Power Cord and Receptacle List

Ref.	Part Number	Description	Feature
-1	806-000001-000	Power cord, AC, North America NEMA 5-15P straight, 125 volts, 10 amps, 3.0 meters Receptacle: NEMA 5-15R	1010
-2	806-000004-001	Power cord, AC, United Kingdom BS 1363 right angle, 250 volts, 10 amps, 2.8 meters Receptacle: BS 1363	1012
-3	806-000005-001	Power cord, AC, European Union CEE 7/7 straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEE 7	1013
-4	806-000006-001	Power cord, AC, Australia AS 3112 straight, 250 volts, 10 amps, 2.8 meters Receptacle: AS 3112	1014
-5	806-000027-000	Power cord, AC, Italy, Chile, Libya, and Ethiopia CEI 23-16/VII straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEI 23-16/VII	1021
-6	806-000029-000	Power cord, AC, Israel SI-32 right angle, 250 volts, 15 amps, 2.8 meters Receptacle: SI-32	1022
-7	806-000030-000	Power cord, AC, Thailand, Philippines, Taiwan, Bolivia, and Peru NEMA 6-15P straight, 250 volts, 15 amps, 2.8 meters Receptacle: NEMA 6-15R	1023
-8	806-000033-000	Power cord, AC, Denmark Afsnit 107-2-D1 straight, 250 volts, 10 amps, 2.8 meters Receptacle: Afsnit 107-2-D1	1024
-9	806-000034-000	Power cord, AC, South Africa, Burma, Pakistan, India, and Bangladesh BS 546 Type, right angle, 250 volts, 15 amps, 2.8 meters Receptacle: BS 546	1025
-10	806-000037-000	Power cord, AC, Switzerland and Liechtenstein SEV 1011 straight, 250 volts, 10 amps, 2.8 meters Receptacle: SEV 1011	1026
-11	806-000038-000	Power cord, AC, United States (Chicago) NEMA 6-15P straight, non-locking, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA 6-15R	1027

Table 6-3 Power Cord and Receptacle List (Continued)

Ref.	Part Number	Description	Feature
-12	806-000040-000	Power cord, AC, United States (Chicago) NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA L6-15R	1028
-13	806-000042-000	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1016 and 1029
-14	806-000043-000	Power cord, AC, Japan NEMA 6-15P straight, 240 volts, 6 amps, 2.8 meters Receptacle: NEMA 6-15R <b>Note:</b> The power cord shipped is specifically intended for use with the associated product and cannot be used with any other electrical products.	1030
-15	806-000058-000	Power cord, AC, Japan JIS 8303 straight, 125 volts, 12 amps, 2.5 meters Receptacle: NEMA 5-15R <b>Note:</b> The power cord shipped is specifically intended for use with the associated product and cannot be used with any other electrical products.	None

An event is a state change, problem detection, or problem correction that requires attention or should be reported to service personnel. An event usually indicates an operational state transition, but may also indicate an impending state change (threshold violation) or provide information only. Events are reported as event codes. This appendix lists three-digit event codes. The codes are listed in numerical order and tabular format as follows:

- **000** through **199** - system events.
- **300** through **399** - fan events.
- **400** through **499** - control processor (CTP) card events.
- **500** through **599** - port events.
- **800** through **899** - thermal sensor events.

Events are recorded in the *Event Log* at the Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface. An event illuminates the system error light-emitting diode (LED) at the product front panel.

Tables in this appendix also provide a:

- **Message** - a text string that describes the event.
- **Severity** - a severity level that indicates event criticality as follows:

- **0** - informational.
- **2** - minor.
- **3** - major.
- **4** - severe (not operational).
- **Explanation** - an explanation of what caused the event.
- **Action** - the recommended course of action (if any) to resolve the problem.
- **Event data** - supplementary event data (if any) that appears in the event log in hexadecimal format.
- **Distribution** - checks in associated fields indicate where the event code is reported (product, management server, or attached host).

## System Events (000 through 199)

Event Code: 011							
Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following an initial machine load (IML) or firmware download, the Login Server database failed cyclic redundancy check (CRC) validation. All fabric service databases initialize to an empty state, resulting in implicit fabric logout of all attached devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓					

Event Code: 021							
Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name Server database failed CRC validation. All fabric service databases initialize to an empty state, resulting in implicit fabric logout of all attached devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓					

Event Code: 031							
Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was rejected with an error. Only requests containing authorized SNMP community names are allowed.						
Action:	Add the community name to the SNMP configuration.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Management Server			Sense Info	Link Incident Log
	✓		Event Log	E-Mail	Call-Home		

Event Code: 051							
Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Management Server database failed CRC validation. All management service databases initialize to an empty state, resulting in implicit logout of all logged-in devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓					

Event Code: 061							
Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the fabric controller database failed CRC validation. All fabric controller databases initialize to an empty state, resulting in momentary loss of interswitch communication.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓					



Event Code: 062							
Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller software detected a path to a director or switch that traverses more than seven interswitch links (hops). This may result in Fibre Channel frames persisting in the fabric longer than timeout values allow.						
Action:	Reconfigure the fabric so the path between any two switches traverses seven or less ISLs.						
Event Data:	Byte 0 = domain ID of the director or switch more than seven hops away.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 063							
Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The director or switch with domain ID indicated in the event data has too many ISLs attached and is unreachable from this switch.						
Action:	Reduce the ISLs on the indicated director or switch to a number within limits specified.						
Event Data:	Byte 0 = domain ID of the director or switch with too many ISLs.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓					

Event Code: 064							
Message:	ESS response from indicated domain ID not received after maximum tries.						
Severity:	Informational.						
Explanation:	Fabric controller software detected an exchange switch support (ESS) response from the indicated domain ID was not received after the maximum attempts. The event is reported only in McDATA interop mode.						
Action:	No action required.						
Event Data:	Byte 0 = domain ID of the director or switch not receiving an ESS response. Byte 1 = domain ID of the director or switch not responding.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 070							
Message:	E_Port is segmented.						
Severity:	Informational.						
Explanation:	An E_Port recognized an incompatibility with the attached director or switch, preventing fabric participation. A segmented port does not transmit Class 2 or Class 3 traffic, but transmits Class F traffic. Refer to event data for segmentation reason.						
Action:	Action depends on segmentation reason specified.						
Event Data:	<p>The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:</p> <p><b>1 = Incompatible operating parameters</b> - Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another director or switch. Modify the R_A_TOV and E_D_TOV to make the values consistent.</p> <p><b>2 = Duplicate domain ID</b> - The switch has the same preferred domain ID as another director or switch) Modify the Domain ID to make it unique.</p> <p><b>3 = Incompatible zoning configurations</b> - The same name is applied to a zone for the switch and another director or switch, but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p><b>4 = Build fabric protocol error</b> - A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform a data collection and return the CD to support personnel.</p> <p><b>5 = No principal switch</b> - No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p><b>6 = No response from attached switch (hello timeout)</b> - The switch periodically verifies operation of attached directors or switches. The E_Port at the operational switch times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform a data collection and return the CD to support personnel.</p>						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 071							
Message:	Switch is isolated.						
Severity:	Informational.						
Explanation:	The switch is isolated from other directors or switches. This event code is accompanied by one or more <b>070</b> event codes. Refer to event data for segmentation reason.						
Action:	Action depends on segmentation reason specified.						
Event Data:	<p>The first byte of event data (byte <b>0</b>) specifies the E_Port number. The fifth byte (byte <b>4</b>) specifies the segmentation reason as follows:</p> <p><b>1 = Incompatible operating parameters</b> - Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another director or switch. Modify the R_A_TOV and E_D_TOV to make the values consistent.</p> <p><b>2 = Duplicate domain ID</b> - The switch has the same preferred domain ID as another director or switch) Modify the Domain ID to make it unique.</p> <p><b>3 = Incompatible zoning configurations</b> - The same name is applied to a zone for the switch and another director or switch, but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p><b>4 = Build fabric protocol error</b> - A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform a data collection and return the CD to support personnel.</p> <p><b>5 = No principal switch</b> - No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p><b>6 = No response from attached switch (hello timeout)</b> - The switch periodically verifies operation of attached directors or switches. The E_Port at the operational switch times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform a data collection and return the CD to support personnel.</p>						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 072							
Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The switch is attached (through an ISL) to an incompatible director or switch.						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 073							
Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, probably caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Byte <b>0</b> = error reason code for engineering evaluation. Bytes <b>4 - 9</b> = port numbers where problems were detected.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 074							
Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (073 event code). Most problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Byte 0 = E_Port number reporting the problem. Bytes 4 - 8 = Count of frame delivery timeouts. Bytes 9 - 11 = Count of frame delivery aborts.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 075							
Message:	E_Port segmentation recovery.						
Severity:	Informational.						
Explanation:	A segmented E_Port (event code 070) recovered. This event is not generated if the port is manually recovered by blocking and unblocking, setting offline and online, or disconnecting the fiber-optic cable.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the original segmentation reason as described in event code 070.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 080							
Message:	Unauthorized worldwide name.						
Severity:	Informational.						
Explanation:	The WWN of the connected device or fabric element is not authorized for the port number.						
Action:	Change the port binding definition or connect the proper device or fabric element to the indicated port.						
Event Data:	Byte 0 = Port number reporting the unauthorized connection. Bytes 4 - 11 = WWN of the unauthorized device or fabric element.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 081	
Message:	Invalid attachment.
Severity:	Informational.
Explanation:	A switch port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to event data for the reason.
Action:	Action depends on reason specified.
Event Data:	<p>The first byte of event data (byte 0) specifies the port number. The fifth byte (byte 4) specifies the isolation reason as follows:</p> <p><b>1 = Unknown</b> - Reason is unknown, but probably caused by failure of an E_Port connected device. Fault isolate the failed device or contact support personnel to report the problem.</p> <p><b>2 = ISL connection not allowed</b> - The port connection conflicts with the configured port type. Change the port type to <b>F_Port</b> if the port is cabled to a device, or <b>E_Port</b> if the port is cabled to a fabric element to form an ISL.</p> <p><b>3 = Incompatible switch</b> - The switch returned a <i>Process ELP Reject - Unable to Process</i> reason code because the attached fabric element is not compatible. Set the switch operating mode to <b>McDATA Fabric 1.0</b> if connected to a McDATA product. Set the switch operating mode to <b>Open Fabric 1.0</b> if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p><b>4 = Incompatible switch</b> - The switch returned a <i>Process ELP Reject - Invalid Revision Level</i> reason code because the attached fabric element is not compatible. Set the switch operating mode to <b>McDATA Fabric 1.0</b> if connected to a McDATA product. Set the switch operating mode to <b>Open Fabric 1.0</b> if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p><b>5 = Loopback plug connected</b> - A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug.</p> <p><b>6 = N_Port connection not allowed</b> - The switch is connected to a fabric element through a misconfigured port. Change the port type to <b>E_Port</b>.</p> <p><b>7 = Non-McDATA switch at other end</b> - The attached fabric element is not a McDATA product. Set the switch operating mode to <b>Open Fabric 1.0</b> if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p><b>8 = E_Port capability disabled</b> - The product does not have E_Port capability. Enable this functionality through the appropriate product feature enablement (PFE) key.</p>



## Event Code: 081 (continued)

Event Data (continued):	<p><b>A = Unauthorized port binding WWN</b> - The device WWN or nickname used to configure port binding for this port is not valid. At the <i>Configure Ports</i> dialog box, reconfigure the port with the WWN or nickname authorized for the attached device, or disable the port binding feature.</p> <p><b>B = Unresponsive node</b> - The attached node did not respond, resulting in a G_Port ELP timeout. Check the status of the attached device and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.</p> <p><b>C = ESA security mismatch</b> - Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The switch binding parameters for this switch and the attached fabric element must agree. At the <i>Switch Binding - State Change</i> dialog boxes, ensure the parameters for both fabric elements are compatible, or disable the fabric and switch binding features.</p> <p><b>D = Fabric binding mismatch</b> - Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. At the <i>Fabric Binding</i> dialog box, update the fabric membership list for both fabric elements to ensure compatibility, or disable the fabric binding feature.</p> <p><b>E = Authorization failure reject</b> - The fabric element connected to the switch through an ISL detected a security violation. As a result, the switch received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.</p> <p><b>F = Unauthorized switch binding WWN</b> - Switch binding is enabled and an attached device or fabric element has an incompatible switch membership list. At the <i>Switch Binding - Membership List</i> dialog box, update the switch membership list for the switch and the attached device or fabric element to ensure compatibility, or disable the switch binding feature.</p> <p><b>10 = Authentication failure</b> - An ISL challenge handshake authentication protocol (CHAP) check failed. Update the authentication list or disable the authentication feature.</p> <p><b>11 = Fabric mode mismatch</b> - Based on the ELP revision level, a connection was not allowed because a McDATA switch in legacy mode is attached to a McDATA switch in Open Fabric mode, or a McDATA switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch using the <i>Interop Mode</i> drop-down list at the <i>Configure Fabric Parameters</i> dialog box.</p>						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓		✓			✓	

Event Code: 082							
Message:	Port fenced.						
Severity:	Informational.						
Explanation:	The port was blocked after exceeding threshold criteria defined by the port fencing policy. A hardware malfunction is indicated or the port fencing policy is too restrictive. The fence type is indicated in the event data.						
Action:	Identify and correct the hardware malfunction (port transceiver, fiber-optic cable, or attached fabric element), or change the port fencing threshold settings to more lenient values. After problem correction, unblock the port.						
Event Data:	<p>The first byte of event data (byte <b>0</b>) specifies the port number. The fifth byte (byte <b>4</b>) specifies the fence type code as follows:</p> <p><b>1 = Protocol error</b> - Failure is associated with persistent incomplete operations or application-layer protocol errors (including port logins, fabric rebuilds, and management protocol errors).</p> <p><b>2 = Link level hot I/O</b> - Failure is hardware related and associated with an unstable link-state machine.</p> <p><b>3 = Security violation</b> - Failure is associated with persistent firmware-related security feature violations (port binding violations or authentication failures).</p> <p>The ninth byte (byte <b>8</b>) specifies the disabled reason code as follows:</p> <p><b>1 = Unknown</b> - The failure reason is unknown.</p> <p><b>9 = ISL fencing</b> - The E_Port (ISL) was fenced after the port exceeded a threshold value.</p>						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓					✓	

Event Code: 083							
Message:	Port set to inactive state.						
Severity:	Informational.						
Explanation:	A hardware or software problem prevented the port from coming online and set the port to an inactive state. Refer to event data for the inactive reason						
Action:	Action depends on inactive reason specified.						
Event Data:	<p>The first byte of event data (byte 0) specifies the port number. The second byte (byte 1) specifies the inactive reason code as follows:</p> <p><b>2 = Feature key not enabled</b> - The optional flexport PFE key is not enabled.</p> <p><b>3 = Switch speed conflict</b> - The port cannot operated at the configured product (backplane or CTP Card) speed.</p> <p><b>4 = Optics speed conflict</b> - The port transceiver does not support the configured port speed.</p> <p><b>5 = No SBAR</b> - A serial crossbar (SBAR) is not installed. Not applicable to 4000-series fabric switches.</p> <p><b>6 = Port swap conflict</b> - The port swap configuration is invalid.</p>						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓					✓	

Event Code: 120							
Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a management command that violates specified boundary conditions, typically as a result of a network error. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 121							
Message:	Zone set activation failed - zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a zone set activation command that exceeds the size supported by the switch. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 140							
Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting congestion.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 141							
Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting congestion relieved.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 142							
Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting low BB_Credit.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 143							
Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting low BB_Credit relieved.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 150							
Message:	Fabric merge failure.						
Severity:	Informational.						
Explanation:	During ISL initialization, the fabric merge process failed. The fabric binding membership lists do not match, an incompatible zone set was detected, there is a problem with exchanging zoning parameters, or the zone set merge failed. This event code is always preceded by a <b>070</b> ISL segmentation event code, and represents the reply of an adjacent fabric element. Refer to the event data for the failure reason.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows:  Bytes <b>0 - 3</b> = Affected E_Port number(s). Bytes <b>4 - 7</b> = Request SW_ILS command codes. Bytes <b>8 - 31</b> = Request response payloads.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓					

Event Code: 151							
Message:	Fabric configuration failure.						
Severity:	Informational.						
Explanation:	A fabric-wide configuration activation process failed. An event code <b>151</b> is recorded only by the managing switch in the fabric. The event code is intended to help engineering support personnel fault isolate a fabric-wide configuration failures.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	<p>Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows:</p> <p>Bytes <b>0 - 3</b> = Managing switch domain ID in internal format (1-31).            Bytes <b>4 - 7</b> = Fabric configuration operation that failed.            Bytes <b>8 - 11</b> = Fabric configuration step that failed.            Bytes <b>12 - 15</b> = Managed switch domain ID in internal format (1-31).            Bytes <b>16 - 19</b> = Response command code received from the managed switch.            Bytes <b>20 - 23</b> = Response code received from the managed switch.            Bytes <b>24 - 27</b> = Reason code received from the managed switch.            Bytes <b>28 - 31</b> = Error code received from the managed switch.</p>						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓					



## Fan Events (300 through 399)

Event Code: 300								
Message:	Cooling fan propeller failed.							
Severity:	Major.							
Explanation:	One cooling fan failed or is rotating at insufficient angular velocity.							
Action:	Replace the switch.							
Event Data:	The first byte of event data (byte 0) specifies the failed fan number.							
Distribution:	Product		Management Server			Host		
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log	
	✓	✓				✓		

Event Code: 301								
Message:	Cooling fan propeller failed.							
Severity:	Major.							
Explanation:	Two cooling fans failed or are rotating at insufficient angular velocity.							
Action:	Replace the switch.							
Event Data:	The first byte of event data (byte 0) specifies the failed fan number(s).							
Distribution:	Product		Management Server			Host		
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log	
	✓	✓				✓		

Event Code: 302							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans failed or are rotating at insufficient angular velocity.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 310							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan recovered.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan number.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 311							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans recovered.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 312							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans recovered						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 370							
Message:	Cooling fan status polling temporarily disabled.						
Severity:	Minor.						
Explanation:	The failed or recovered status values for one or more cooling fans are exceeding a determined threshold. This indicates a possible fan failure. Fan status polling is enabled hourly or following an IML or reset.						
Action:	No immediate action required. Monitor cooling fan operation or additional event codes indicating a fan failure.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓					

## CTP Card Events (400 through 499)

Event Code: 400							
Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a failed FRU as indicated by the event data.						
Action:	If a CTP card, fan, or power supply failure is indicated, replace the switch. Perform a data collection and return the CD to support personnel.						
Event Data:	Byte 0 = FRU code as follows: <b>02</b> = CTP card, <b>05</b> = cooling fan, <b>06</b> = power supply assembly. Byte 1 = FRU slot number.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 410							
Message:	Switch reset.						
Severity:	Informational.						
Explanation:	The switch reset due to system power-up, IML, or manual reset. A software reset can occur automatically after a firmware fault (event code <b>411</b> ), or be user-initiated. Event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte 0 = reset type as follows: <b>00</b> = power-on, <b>02</b> = IML, <b>04</b> = reset.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 411							
Message:	Firmware fault.						
Severity:	Major.						
Explanation:	Switch firmware encountered an unexpected condition and dumped operating state information to FLASH memory for retrieval and analysis. The dump file automatically transfers to the management server, where it is stored for retrieval through a data collection. The switch performs a software reset, during which all attached Fibre Channel devices are momentarily disrupted, log out, and log back in.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Bytes 0 - 3 = fault identifier, least significant byte first.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 412							
Message:	CTP watchdog timer reset.						
Severity:	Informational.						
Explanation:	The hardware watchdog timer expired and caused the CTP card to reset.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Byte 0 = reset type as follows: 00 = task switch did not occur within approximately one second, 01 = interrupt servicing blocked for more than approximately one second.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 421							
Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A new firmware version was downloaded from the management server or EFCM Basic interface. Event data contains the ASCII firmware version in hexadecimal format <b>xx.yy.zz.bbbb</b> .						
Action:	No action required.						
Event Data:	Bytes 0 and 1 = release level ( <b>xx</b> ).		Bytes 6 and 7 = interim release level ( <b>zz</b> ).				
	Byte 2 = always a period.		Byte 8 = always a space.				
	Bytes 3 and 4 = maintenance level ( <b>yy</b> ).		Bytes 9 - 12 = build ID ( <b>bbbb</b> ).				
	Byte 5 = always a period.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 423							
Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The management server or EFCM Basic Edition interface initiated download of a new firmware version.						
Action:	No action required.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 426							
Message:	Multiple ECC single-bit errors occurred.						
Severity:	Minor.						
Explanation:	When the SDRAM controller detects an error checking and correction (ECC) error, an interrupt occurs. If an interrupt occurs a certain number of times weekly, a <b>426</b> event code is recorded. The number of interrupts is indicated by the event data.						
Action:	No action required. SDRAM is probably malfunctioning intermittently.						
Event Data:	Byte <b>0</b> of the event data (equal to <b>5</b> , <b>10</b> , <b>15</b> , or <b>20</b> ) is recorded. The number of interrupts equals two to the power of the event data. Event data equal to <b>10</b> indicates 1,024 ECC error interrupts.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 433							
Message:	Nonrecoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable Ethernet interface failure was detected and the LAN connection to the management server or Internet was terminated. No failure information or event codes are reported outside the switch. Although Fibre Channel port functionality is not affected, the switch cannot be monitored or configured.						
Action:	Replace the switch.						
Event Data:	Byte <b>0</b> = LAN error type as follows: <b>01</b> = hard failure, <b>04</b> = registered fault. Byte <b>1</b> = LAN error subtype (internally defined). Byte <b>2</b> = LAN fault identifier (internally defined).						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	



Event Code: 440							
Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal error.						
Action:	Replace the switch.						
Event Data:	Byte 0 = CTP slot position (00). Byte 1 = engineering reason code Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 442							
Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte 0 = embedded port number. Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = HA error callout #1. Bytes 10 and 11 = HA error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = HA error callout #3. Bytes 18 and 19 = HA error callout #4.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 445							
Message:	ASIC detected a system anomaly.						
Severity:	Informational.						
Explanation:	The application-specific integrated chip (ASIC) detected a deviation in the normal operating mode or operating status of the switch.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold that results in a system event.						
Event Data:	Byte 0 = embedded port number. Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = HA error callout #1. Bytes 10 and 11 = HA error callout #2.			Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = HA error callout #3. Bytes 18 and 19 = HA error callout #4.			
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 453							
Message:	New feature key installed.						
Severity:	Informational.						
Explanation:	This event occurs when a new feature key is installed from the management server or EFCM Basic Edition interface. The switch performs an IPL when the feature key is enabled. Event data indicates the feature(s) installed.						
Action:	No action required.						
Event Data:	Byte 0 = feature description as follows: 00 - 04 = flexport technology, 06 = open systems management server, 07 = FICON management server. Byte 1 = feature description as follows: 01 = full volatility, 02 = FICON cup zoning, 03 = SANtegrity authentication, 05 = hardware trunking, 06 = SANtegrity binding, 07 = open trunking.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

## Port Events (500 through 599)

Event Code: 506							
Message:	Fibre Channel port failure.						
Severity:	Major.						
Explanation:	A Fibre channel port failed. The amber LED corresponding to the port illuminates to indicate the failure. Ports with LEDs extinguished remain operational.						
Action:	Perform a a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	Byte 0 = port number. Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = reason code specific. Byte 16 = connector type.			Bytes 17 and 18 = transmitter technology. Byte 19 = distance capability. Byte 20 = supported transmission media. Byte 21 and 22 = speed capability.			
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 507							
Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code <b>506</b> is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte 0 = port number. Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count.			Bytes 8 - 11 = reason code specific. Byte 12 = test type.			
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 508							
Message:	Fibre Channel port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.						
Action:	No action required. An event code <b>506</b> is generated if this anomaly results in a hard port failure.						
Event Data:	Byte 0 = port number. Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = HA error callout #1. Bytes 10 and 11 = HA error callout #2.			Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = HA error callout #3. Bytes 18 and 19 = HA error callout #4.			
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 510							
Message:	Optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of an optical transceiver was initiated with the switch powered on and operational. The event indicates operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte 0 = port number. Byte 2 = optic type. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 512							
Message:	Optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Switch firmware detected an optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number. Byte 1 = engineering reason code. Byte 2 = optic type. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 513							
Message:	Optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An optical transceiver was removed while the switch was powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = port number. Byte 2 = optic type. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 514							
Message:	Optical transceiver failure.						
Severity:	Major.						
Explanation:	An optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Ports with LEDs extinguished remain operational.						
Action:	Replace the failed transceiver.						
Event Data:	Byte 0 = port number. Byte 1 = engineering reason code. Byte 2 = optic type. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 515							
Message:	Optical digital diagnostics warning threshold exceeded.						
Severity:	Minor.						
Explanation:	An optical transceiver digital diagnostics warning threshold was exceeded. Additional event code 515 events are recorded if the problem persists.						
Action:	Replace the transceiver.						
Event Data:	Byte 0 = port number. Byte 2 = optic type. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 31 = First, second, and third type (and threshold value) of warning threshold exceeded as follows: 01 = TX temperature, 02 = TX supply voltage, 03 = TX bias current, 04 = TX power, 05 = RX power.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 516							
Message:	Optical digital diagnostics alarm threshold exceeded.						
Severity:	Minor.						
Explanation:	An optical transceiver digital diagnostics alarm threshold was exceeded. Additional event code <b>516</b> events are recorded if the problem persists.						
Action:	Replace the transceiver.						
Event Data:	Byte 0 = port number. Byte 2 = optic type. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 31 = First, second, and third type (and threshold value) of warning threshold exceeded as follows: <b>01</b> = TX temperature, <b>02</b> = TX supply voltage, <b>03</b> = TX bias current, <b>04</b> = TX power, <b>05</b> = RX power.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 523							
Message:	FL_Port open request failed.						
Severity:	Informational.						
Explanation:	When the indicated FL_Port attempted to open a loop device, a port open (OPN) sequence was returned.						
Action:	No action required.						
Event Data:	Byte 0 = port number. Byte 1 = arbitrated loop physical address (AL_PA) of the device transmitting the OPN sequence.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 524							
Message:	No AL_PA acquired.						
Severity:	Informational.						
Explanation:	Switch cannot allocate an AL_PA of 0 (loop master) during loop initialization. The device cannot participate in loop operation.						
Action:	Disconnect the loop master FC-AL device.						
Event Data:	Byte 0 = port number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						

Event Code: 525							
Message:	FL_Port arbitration timeout.						
Severity:	Informational.						
Explanation:	A switch port could not win loop arbitration within the specified loop protocol time out value (LP_TOV).						
Action:	Switch firmware reinitializes the arbitrated loop. No action required.						
Event Data:	Byte 0 = port number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓						



Event Code: 581							
Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to <a href="#">MAP 0000: Start MAP</a> to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✓

Event Code: 582							
Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	An attached server determined the number of code violation errors recognized exceeded the bit error threshold.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to <a href="#">MAP 0000: Start MAP</a> to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✓

Event Code: 583							
Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to <a href="#">MAP 0000: Start MAP</a> to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✓

Event Code: 584							
Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached server received a not-operational primitive sequence (NOS).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to <a href="#">MAP 0000: Start MAP</a> to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✓

Event Code: 585							
Message:	Primitive sequence timeout.						
Severity:	Major.						
Explanation:	An attached server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was not longer recognized).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to <a href="#">MAP 0000: Start MAP</a> to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✓

Event Code: 586							
Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	An attached server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to <a href="#">MAP 0000: Start MAP</a> to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✓

## Thermal Sensor Events (800 through 899)

Event Code: 810							
Message:	High temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the CTP card indicates the warm temperature threshold was reached or exceeded.						
Action:	Perform a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 811							
Message:	Critically hot temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the CTP card indicates the hot temperature threshold was reached or exceeded.						
Action:	Perform a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCMBasic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 812							
Message:	CTP card shutdown due to thermal violations.						
Severity:	Major.						
Explanation:	The CTP card failed due to excessive thermal violations. This event follows an event code 811.						
Action:	Perform a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	

Event Code: 850							
Message:	Switch shutdown due to CTP thermal violations.						
Severity:	Severe.						
Explanation:	The switch failed due to excessive CTP card thermal violations.						
Action:	Perform a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✓	✓				✓	



**A**

AC power receptacle, location [1-3](#)  
attention statements [xviii](#)

**B**

back up switch configuration file [4-24](#)  
BB\_Credit  
    configure [2-15](#)  
    description [2-15](#)  
block port [4-20](#)

**C**

clean fiber-optic components [4-4](#)  
clearances [1-6](#)  
command line interface  
    disable [2-17](#)  
    enable [2-17](#)  
compliance statements  
    Argentinian IRAM Certification [xvi](#)  
    Australia C-Tick Mark [xvi](#)  
    Canadian EMC [xiv](#)  
    CB Scheme [xv](#)  
    Chinese BSMI Statement [xvii](#)  
    Chinese CCC Mark [xvii](#)  
    Class 1 laser transceiver [xiv](#)  
    European Union CE Mark [xv](#)  
    European Union N-Mark [xvi](#)  
    Federal Communications Commission [xiv](#)  
    German TÜV GS Mark [xvii](#)  
    Japanese VCCI Statement [xvii](#)  
    Korean MIC Mark [xviii](#)  
    Mexican NOM Mark [xviii](#)

    new Zealand C-Tick Mark [xvi](#)  
    Russian GOST Certification [xviii](#)  
    UL Certification [xiv](#)  
configuration file  
    back up [4-24](#)  
    restore [4-24](#)  
configure  
    basic port information [2-14](#)  
    fabric parameters [2-11](#)  
    ISL performance features [2-22](#)  
    OSMS [2-18](#)  
    PFE keys [2-20](#)  
    port BB\_Credit [2-15](#)  
    port fencing [2-22](#)  
    port NPIV [2-16](#)  
    preferred path [2-22](#)  
    SNMP [2-16](#)  
    SSL encryption  
        software [2-19](#)  
        web [2-19](#)  
    switch date and time [2-8](#)  
    switch identification [2-7](#)  
    switch network information [2-12, 2-23](#)  
    switch operating parameters [2-9](#)  
    zone sets [2-27](#)  
    zones [2-26](#)  
cooling fan  
    description [1-4](#)  
    events (300 - 399) [A-21](#)  
    fault isolation [3-14](#)  
CTP card  
    events (400 - 499) [A-25](#)  
    fault isolation [3-14](#)  
    firmware versions [4-21](#)

**D**

- danger statements [xviii](#)
- data collection procedure [4-18](#)
- date (set switch date) [2-8](#)
- default
  - EFCM Basic Edition
    - password [2-6](#)
    - user name [2-6](#)
  - maintenance port password [2-25](#), [3-13](#)
  - switch
    - gateway address [2-1](#), [3-1](#)
    - IP address [2-1](#), [3-1](#)
    - passwords [2-1](#), [3-1](#)
    - subnet mask [2-1](#), [3-1](#)
- dimensions [1-6](#)
- door key
  - description [1-10](#)
  - illustration [1-10](#)
- download firmware
  - from filecenter [4-6](#)
  - from PC hard drive [4-22](#)

**E**

- E\_D\_TOV [2-11](#)
- E\_Port
  - configure [2-14](#)
  - description [1-2](#)
  - enable through PFE key [2-20](#)
  - performance features [2-22](#)
  - port fencing [2-22](#)
  - preferred path [2-22](#)
  - segmented [3-29](#)
- EFCM Basic Edition
  - configure product [2-6](#)
  - embedded port frame log [4-11](#)
  - event log [4-10](#)
  - fabric log [4-11](#)
  - link incident log [4-10](#)
  - open trunking re-route log [4-10](#)
- embedded port frame log [4-11](#)
- enable
  - command line interface [2-17](#)
  - host control [2-18](#)
  - SSL encryption
    - software [2-19](#)
    - web [2-19](#)

**environment**

- operating [1-7](#)
- shipping [1-7](#)
- storage [1-7](#)

**ERR LED**

- description [1-5](#)
- location [1-2](#)

**error detection**

- description [1-8](#)
- event codes [3-2](#)

**error reporting**

- description [1-8](#)
- event codes [3-2](#)

**ESD**

- precautions [xxi](#)
- RRP precautions [5-2](#)

**Ethernet connector**

- description [1-5](#)
- location [1-2](#)

**event codes**

- cooling fan events (300 - 399) [A-21](#)
- CTP card events (400 - 499) [A-25](#)
- description [A-1](#)
- port events (500 - 599) [A-31](#)
- system events (000 - 199) [A-2](#)
- thermal sensor events (800 - 899) [A-40](#)

**event log [4-10](#)****external loopback test [4-17](#)****F****F\_Port**

- configure [2-14](#)
- description [1-1](#)

**fabric log [4-11](#)****fabric parameters (configure) [2-11](#)****Fabriccenter equipment cabinet**

- description [1-2](#)
- switch installation [2-5](#)

**fault isolation**

- MAP 0000 - Start MAP [3-5](#)
- MAP 0100 - Power distribution analysis [3-9](#)
- MAP 0200 - POST failure analysis [3-10](#)
- MAP 0300 - Loss of browser PC communication [3-11](#)
- MAP 0400 - FRU failure analysis [3-14](#)



- MAP 0500 - Port failure or link incident
  - analysis [3-16](#)
- MAP 0600 - Fabric or ISL problem
  - analysis [3-27](#)
  - summary [3-2](#)
- fenced E\_Port
  - description [3-33](#)
  - fault isolation [3-27](#)
- fiber-optic protective plug
  - description [1-10](#)
  - illustration [1-10](#)
- filecenter (download firmware) [4-6](#)
- firmware
  - determine version [4-22](#)
  - download from filecenter [4-6](#)
  - download from PC hard drive [4-22](#)
- FL\_Port
  - configure [2-14](#)
  - description [1-2](#)
- Flexport Technology
  - configure PFE key [2-20](#)
  - description [2-20](#)
- FRU removal
  - SFP transceiver [5-3](#)
  - tools required [5-3](#)
- FRU replacement
  - SFP transceiver [5-4](#)
  - tools required [5-3](#)
- FRUs
  - description [1-2](#)
  - illustrated parts breakdown [6-1](#)
  - SFP transceiver [1-3](#)
  - status LEDs [1-5](#)
- full-fabric capability
  - configure PFE key [2-20](#)
  - description [2-20](#)
- full-volatility feature
  - configure PFE key [2-20](#)
  - description [4-18](#)

## G

- gateway address
  - change switch address [2-12, 2-23](#)
  - switch default [2-1, 3-1](#)

## I

- illustrated parts breakdown
  - front-accessible FRUs [6-2](#)
  - miscellaneous parts [6-3](#)
  - power cords [6-4](#)
- IML switch [4-4](#)
- IML/RESET button
  - function [1-4](#)
  - location [1-2](#)
- insistent domain ID [2-9](#)
- installation tasks
  - summary [2-2](#)
  - Task 1 - Verify installation requirements [2-2](#)
  - Task 2 - Unpack, inspect, and install the product [2-3](#)
  - Task 3 - Configure product at the EFCM Basic Edition interface [2-6](#)
  - Task 4 - Configure product network information (optional) [2-23](#)
  - Task 5 - Cable Fibre Channel ports [2-26](#)
  - Task 6 - Configure zoning (optional) [2-26](#)
  - Task 7 - Connect product to a fabric element (optional) [2-27](#)
  - Task 8 - Register with the McDATA file center [2-28](#)
- internal loopback test [4-15](#)
- interop mode [2-12](#)
- interswitch link
  - configure performance features [2-22](#)
  - description [1-2](#)
  - fault isolation [3-27](#)
  - port fencing [2-22](#)
  - preferred path [2-22](#)
- IP address
  - change switch address [2-12, 2-23](#)
  - switch default [2-1, 3-1](#)

## L

- laser transceiver
  - compliance statement [xiv](#)
  - description [1-3](#)
  - illustrated parts breakdown [6-2](#)
  - removal [5-3](#)
  - replacement [5-4](#)
  - types available [1-3](#)

## LEDs

- ERR 1-5
- port status 1-5
- power supply status 1-5
- PWR 1-5

link incident log 4-10

## logs

- embedded port frame 4-11
- event 4-10
- fabric 4-11
- link incident 4-10
- open trunking re-route 4-10

## loopback plug

- description 1-10
- illustration 1-10

## loopback test

- external 4-17
- internal 4-15

## M

MAC address, switch 2-23

## maintenance analysis procedures

- MAP 0000 - Start MAP 3-5
- MAP 0100 - Power distribution analysis 3-9
- MAP 0200 - POST failure analysis 3-10
- MAP 0300 - Loss of browser PC communication 3-11
- MAP 0400 - FRU failure analysis 3-14
- MAP 0500 - Port failure or link incident analysis 3-16
- MAP 0600 - Fabric or ISL problem analysis 3-27
- summary 3-2

maintenance approach 1-7

## maintenance port

- configure switch network addresses 2-23
- default password 2-25, 3-13
- description 1-6
- location 1-3

manage configuration data 4-23

## N

network information (configure switch) 2-12, 2-23

## NPIV

- configure 2-16
- description 2-16

## null modem cable

- description 1-11
- illustration 1-11

## O

open trunking re-route log 4-10

## open-systems management server

- configure 2-18
- description 2-18

operating environment 1-7

operating parameters (configure) 2-9

## P

## password

- customer-level switch 2-1, 3-1
- default EFCM Basic Edition 2-6
- default maintenance port 2-25, 3-13
- maintenance-level switch 2-1, 3-1

## PFE keys

- configure 2-20
- Flexport Technology 2-20
- full-fabric capability 2-20
- full-volatility 2-20

## port fencing

- configure 2-22
- description 2-22

## ports

- cabling 2-26
- configurable types 1-1
- configure basic information 2-14
- configure BB\_Credit 2-15
- configure NPIV 2-16
- E\_Port fencing 2-22
- events (500 - 599) A-31
- LED diagnostics 4-8
- SFP transceivers 1-3
- status LEDs 1-5

## power cords

- description 6-4
- illustrated parts breakdown 6-4

power requirements 1-6

power supply  
 description 1-4  
 fault isolation 3-9  
 status LED 1-5

power-off procedure 4-3

power-on procedure 4-2

precautions  
 ESD [xxi](#)  
 general [xxi](#)

preferred domain ID 2-10

preferred path  
 configure 2-22  
 description 2-22

procedural notes 4-1

procedures  
 block or unblock port 4-20  
 data collection 4-18  
 installation 2-2  
 manage configuration data 4-23  
 obtain log information 4-9  
 power-off 4-3  
 power-on 4-2  
 repair 4-1  
 set online state 4-19  
 upgrade firmware 4-21

publications, related [xii](#)

PWR LED  
 description 1-5  
 location 1-2

**R**

R\_A\_TOV 2-11

rack-mount installation (switch) 2-5

related publications [xii](#)

remove and replace procedures  
 ESD precautions 5-2  
 FRU list 5-2  
 procedural notes 5-1

repair procedures  
 block or unblock port 4-20  
 clean fiber-optic components 4-4  
 collect maintenance data 4-18  
 download firmware 4-6  
 IML or reset switch 4-3

manage configuration data 4-23

obtain log information 4-9

overview 4-1

port LED diagnostics 4-8

power-off procedure 4-3

power-on procedure 4-2

set online state 4-19

upgrade firmware 4-21

rerouting delay 2-10

reset  
 configuration data 4-25  
 switch 4-4

restore switch configuration file 4-24

## S

safety  
 attention statements [xviii](#)  
 danger statements [xviii](#)  
 ESD precautions [xxi](#), 5-2  
 general precautions [xxi](#)

segmented E\_Port  
 description 3-29  
 fault isolation 3-27

serviceability features 1-8

set online state 4-19

SFP transceiver  
 description 1-3  
 fault isolation 3-16  
 illustrated parts breakdown 6-2  
 removal 5-3  
 replacement 5-4  
 types available 1-3

shipping environment 1-7

SNMP  
 configure 2-16  
 description 2-16

solution center  
 e-mail address [xiii](#)  
 fax number [xiii](#)  
 phone number [xiii](#)

specifications  
 switch clearances 1-6  
 switch dimensions 1-6  
 switch power requirements 1-6

Sphereon 4300 Fabric Switch  
description 1-1  
FRU removal and replacement 5-1  
FRUs 1-2  
illustrated parts breakdown 6-1  
installation 2-3  
maintenance approach 1-7  
management 1-8  
repair procedures 4-1  
specifications 1-6

SSL encryption  
configure software encryption 2-19  
configure web encryption 2-19

storage environment 1-7

subnet mask  
change switch value 2-12, 2-23  
switch default 2-1, 3-1

switch priority 2-11

system events (000 - 199) A-2

## T

technical support  
e-mail address xiii  
fax number xiii  
phone number xiii

thermal sensor events (800 - 899) A-40

time (set switch time) 2-8

tools and test equipment  
FRU removal and replacement 5-3  
supplied by service personnel 1-11  
supplied with product 1-10

trademarks xiii

## U

unblock port 4-20

user name (default EFCM Basic Edition) 2-6

## V

verify SFP transceiver replacement 5-5

## Z

zone sets  
configure 2-27  
description 2-27  
naming conventions 2-27

zones  
configure 2-27  
description 2-26  
naming conventions 2-27